Probabilistische Grundlage zur Darstellung integraler Mehrzustands-Fehlermodelle komplexer technischer Systeme

Vom Fachbereich Maschinenbau
an der Technischen Universität Darmstadt
zur
Erlangung des Grades eines Doktor-Ingenieurs (Dr.-Ing.)
genehmigte

Dissertation

vorgelegt von

Dipl.-Ing. Matthias Rauschenbach
aus Augsburg

Berichterstatter:	Prof. Dr.-Ing. Tobias Melz
Mitberichterstatter:	Prof. Dr.-Ing. Uwe Klingauf
Tag der Einreichung:	02. Mai 2017
Tag der mündlichen Prüfung:	12. Juli 2017

Darmstadt 2017

D17

Danksagung

Diese Arbeit entstand begleitend zu meiner Tätigkeit als wissenschaftlicher Mitarbeiter am Fraunhofer-Institut für Betriebsfestigkeit und Systemzuverlässigkeit LBF.

Ich danke Herrn Prof. T. Melz vom Fachgebiet Systemzuverlässigkeit und Maschinenakustik an der TU Darmstadt und ebenso seinem Vorgänger, Herrn Prof. H. Hanselka, für das Vertrauen und die Zustimmung zur Betreuung dieser Arbeit als Doktorvater.

Herrn Prof. U. Klingauf vom Fachgebiet Flugsysteme und Regelungstechnik der TU Darmstadt danke ich sehr herzlich für das Interesse an der Arbeit und die Übernahme des Korreferats.

Herrn Prof. Th. Bein danke ich sehr für seinen Zuspruch und die Unterstützung von Aktivitäten in diesem Arbeitsgebiet, aus welchen die Themenstellung für diese Arbeit hervorging.

Mein ganz besonderer Dank gilt Herrn Dr. J. Nuffer für die Unterstützung und wertvollen Ratschläge begleitend zur Umsetzung dieser Arbeit, sowie für die sehr gute und angenehme Zusammenarbeit. Seine beispielhafte Geduld durfte ich gelegentlich umfassend in Anspruch nehmen.

Nicht zuletzt danke ich meinen lieben Eltern und der geliebten Frau in meinem Leben für den liebevollen Beistand und den bedingungslosen Rückhalt - danke für alles.

Darmstadt, im April 2017

Nicht auf mich, sondern auf den Logos hörend,
ist es weise, anzunehmen, dass alles eins ist.

(Heraclitos von Ephesos)

Kurzfassung

Begleitend zur Entwicklung technischer Systeme, insbesondere solcher mit hohen Anforderungen an Qualität, Zuverlässigkeit und Sicherheit, ist die Anwendung methodischer Fehleranalysen gebräuchlich und zweckdienlich. Die Ansätze der Fehlermöglichkeits- und Einflussanalyse (FMEA), Fehlerbaumanalyse (FTA) und Zuverlässigkeitsblockdiagramme (RBD) basieren auf einem gemeinsamen Grundkonzept, nach welchem die Funktionsfähigkeit oder mögliche Fehlzustände des Systems in Abhängigkeit von Fehlern der Komponenten dargestellt werden. Dies hat zum Zweck, Risiken oder Fehlerwahrscheinlichkeiten einzuschätzen. Die Systematiken dieser Methoden unterliegen dabei spezifischen Einschränkungen, sodass entweder keine quantitative Auswertung (FMEA), keine Differenzierung verschiedenartiger Fehlzustände (RBD) oder keine zusammenhängende Gesamtabbildung des Systems (FTA) darstellbar ist. So wurden Ansätze veröffentlicht, die auf differenziertere Mehrzustandsbetrachtungen in den Fehlermodellen von FTA und RBD abzielen. Diese sind jedoch nur in begrenztem Umfang praktikabel. Ansätze, FMEA-Fehlermodelle algebraisch zu formalisieren und quantitativ auszuwerten, erreichten dieses Ziel bislang nur partiell.

Die Arbeit setzt in diesem Problemfeld mit dem Ziel an, die algebraische Grundlage zu erarbeiten und einen Modellansatz zu definieren, um quantitative sowie hinsichtlich funktionsfähigkeits- und zuverlässigkeitsbezogener Komponentenzustände differenzierte komplexe Fehlermodelle darstellen und berechnen zu können. Dazu wird eine integrale mengentheoretische Betrachtungsweise der Zustandsmöglichkeiten systemischer Komponentenverbünde auf Basis der Zustandsmöglichkeiten der zugehörigen Bauteile aufgebaut. Auf dieser Grundlage wird eine logisch-algebraische Interpretation konsistenter Ursache-Folge-Beziehungsnetzwerke und deren probabilistische Auswertung hergeleitet und deren Umsetzung am Beispiel Bayesscher Netzwerke aufgezeigt.

Die so erarbeiteten Erkenntnisse dienen anschließend der Ableitung einer methodischen Systematik zum Aufbau komplexer probabilistischer Fehlermodell-Netzwerke für Systeme mit mehreren Hierarchieebenen der enthaltenen Unterbestandteile. Dies erfolgt innerhalb eines Rahmenkonzepts für integrale System-Fehlermodelle, das anhand der klassischen Methoden abgeleitet wird. Die praktische Anwendung wird abschließend anhand exemplarischer Fallbeispiele diskutiert. Dabei wird gezeigt, inwieweit dieses Konzept die Beschreibung komplexer Zustandsbeziehungen erlaubt, die mit gebräuchlichen Methoden nicht entsprechend abbildbar sind. Ausblickend werden Möglichkeiten zur praxisgerichteten Optimierung der Umsetzung des Modellierungsverfahrens prinzipiell aufgezeigt.

Abstract

Along with the development of technical systems, especially such with high requirements concerning quality, reliability and safety, the application of methodical failure analysis is common and beneficial. The approaches of Failure Modes and Effects Analysis (FMEA), Fault Tree Analysis (FTA) and Reliability Block Diagrams (RBD) are based on a common fundamental principle, according to which the ability to function or possible failure states of the system are represented in dependence on possible failure modes of its components. Subsequently, risks or the probabilities of failures are to be assessed. The systematics of those methods underlie specific restrictions, for which either no quantitative evaluation is enabled (FMEA) or no differentiation of dissimilar failure modes (RBD) or no coherent model of an entire system (FTA) is possible to be generated. Hence, approaches were published, which aim at a more differentiated multi-state perspective in the failure models of FTA or RBD. Their practical usability is rather restricted. Approaches formalizing FMEA-failure-models in an algebraic way only partially reached this goal.

Located in this area of problems this work´s projection is to establish the algebraic foundation and define an approach to enable the arrangement and calculation of differentiated complex failure models on a quantitative basis and differentiated concerning the component´s ability to function and their reliability. For this an integral set-theoretic perspective of possible states of a systemic assemblage of components is being elaborated based on the possible states of the parts it consists of. Subsequently, a logical algebraic interpretation of consistent cause-effect-relation networks and their probabilistic evaluation are being deduced as well as their implementation investigated using Bayesian Networks exemplarily.

The findings worked out thereby subsequently serve for the derivation of a methodological scheme for the establishment of complex probabilistic failure model networks for systems with multiple hierarchical levels of the contained sub-entities and components. This is carried out within a framework concept for integral system-failure models, which is derived from the classical methods. Along with this it is being shown, in how far this concept allows for a description of complex relation between states, which is not accordingly possible with common methods. As an outlook, possibilities for an optimization concerning the practical application of the modeling approach are being indicated in their principle.

Inhaltsverzeichnis

Nomenklatur

lateinische Buchstaben:

$\mathcal{A}$	exhaustiv partitionierte Menge
DC	Diagnosedeckungsgrad (aus dem Englischen: „Diagnostic Coverage Factor", DC)
e	Eulersche Zahl
F	Funktionswahrscheinlichkeit
P	Wahrscheinlichkeit
R	Zuverlässigkeit

griechische Buchstaben:

δ	bedingte Übergangswahrscheinlichkeit in Ursache-Folge-Relationen
λ	Ausfallrate
Ω	totale Wahrscheinlichkeit, universeller Wahrscheinlichkeitsraum
$\Omega_{IJ\ldots}$	Teil-Wahrscheinlichkeitsraum bezüglich der Zufallsgrößen I, J, …

aussagenlogische Symbole und Operatoren:

$\cup$	Disjunktion, inklusiv (ODER-Operator)
$\underline{\cup}$	Disjunktion, exklusiv (XODER-Operator)
$\bigcup_i$	Disjunktion, inklusiv, Rekursionsterm
$\underline{\bigcup_i}$	Disjunktion, exklusiv, Rekursionsterm
$\setminus$	Exklusion (OHNE-Operator)
^{c}	Komplement
$\cap$	Konjunktion (UND-Operator)
$\bigcap_i$	Konjunktion, Rekursionsterm
$\{\}$	leere Menge
$-$	Negation (NICHT-Operator)
$\rightarrow$	Zuordnung von Mengenelementen

arithmetische Symbole und Operatoren:

$\otimes$	kartesisches Produkt
$\prod_i$	Produkt, Rekursionsterm
$\sum_i$	Summe, Rekursionsterm

Abkürzungen

BN	Bayessches Netzwerk
BN-FMEA	FMEA auf Basis von Bayesschen Netzwerken
CC-Fehler	Fehler gemeinsamer Ursache (englisch: Common-Cause-Failure)
CPT	Tabelle bedingter Abhängigkeiten (englisch: Conditional Probability Table)
dBN	Dynamisches Bayessches Netzwerk
ETA	Ereignisbaumanalyse (Event Tree Analysis)
FMEA	Fehlermöglichkeits- und Einfluassanalyse (Failure Mode and Effects Analysis)
FN	Fehlernetz
FN-FMEA	FMEA auf Basis von Fehlernetzen
FTA	Fehlerbaumanalyse (Fault Tree Analysis)
i.O.	in Ordnung
pFMEA	probabilistische FMEA (nach [Grunske07])
probFMEA	probabilistische FMEA (nach [Kaiser15])
RBD	Zuverlässigkeitsblockdiagramm (Reliability Block Diagram)

Das, wobei unsere Berechnungen versagen,
nennen wir Zufall.

(Albert Einstein)

1 Einleitung

Bei der Entwicklung technischer Systeme gilt es vorrangig, die erwünschten Eigenschaften eines Produkts durch dessen geeignete technische Gestaltung zu erzielen. Doch ist es dabei nicht minder wichtig, auch unerwünschte Eigenschaften und Defekte durch geeignete Konzeption und Auslegung auszuschließen. So können beispielsweise Defekte, die auf eine nicht ausreichende Beanspruchbarkeit oder zu geringe Langlebigkeit einzelner Komponenten zurückzuführen sind, letztlich einen frühzeitigen Ausfall, einen partiellen Funktionsverlust, ein Fehlverhalten oder eine qualitative Verschlechterung von Systemeigenschaften verursachen.

Das Erreichen der Funktionsfähigkeit kann in der Regel durch Verifikation der beabsichtigten Produkteigenschaften überprüft werden. Dies geschieht vorzugsweise sowohl hinsichtlich des grundsätzlichen Verhaltens des Produkts als auch im Hinblick auf die Erhaltung der erwünschten Eigenschaften für eine ausreichende Einsatzdauer und unter Berücksichtigung typischer Randbedingungen. Jedoch ist die Überprüfung hinsichtlich selten beobachtbarer Fehler, wie beispielsweise solcher, die nur unter besonderen Bedingungen auftreten, sowie jener, die von einer ausreichenden Aufrechterhaltung aller für die Funktionsfähigkeit notwendiger Eigenschaften abhängen, von besonderer Ungewissheit behaftet.

Hintergrund für die Arbeit ist der gebräuchliche Ansatz der methodischen Analyse und Bemessung der Ursächlichkeiten, die ein ungeeignetes Verhalten und Fehler im Produkt bewirken können. Hierfür werden Methoden zur systematischen Fehleranalyse eines Produkts angewandt, die als Ergänzung zu den primären Entwicklungsaktivitäten dienen, um potenzielle Fehlerquellen zu identifizieren und deren Auswirkungen möglichst objektiv zu beurteilen. Als quantitatives Maß wird dabei die Wahrscheinlichkeit verwendet, mit der Fehler in Komponenten auftreten und als Folge bestimmte Fehlzustände des Systems verursachen können. So sollen durch die Analyse und Bewertung möglicher Fehlerursachen und deren Folgen besonders kritische Probleme gegenüber weniger schwerwiegenden hervorgehoben oder Aussagen über die Zuverlässigkeit des Produkts erarbeitet werden.

Im Laufe der vergangenen Jahrzehnte wurden verschiedene solcher Analysemethoden entwickelt. Einige dieser Methoden sind im heutigem Stand von Wissenschaft und Technik fest etabliert und werden in zahlreichen Branchen- und Anwendungsfeldern zum Teil obligatorisch verwendet, wie beispielsweise in Luft- und Raumfahrt, Schienentransporttechnik, Prozessindustrie und Anlagenbau, Automobilbau, Fertigungstechnik, Reaktortechnik, Medizintechnik, allgemeiner Sicherheitstechnik sowie zahlreichen weiteren.

1.1 Ausgangssituation und Problemstellung

Die Fehlermöglichkeits- und Auswirkungsanalyse (FMEA) wird einer Studie [Leyendecker08] zufolge von rund 45 % der untersuchten Betriebe verwendet und stellt die meistgenutzte Methodik zur Fehleranalyse dar [Ehrlenspiel09]. Gemäß deren Methodik werden mögliche Beziehungen zwischen Fehlerursachen in Bauteilen und deren Auswirkungen für die Systemfunktion ermittelt und beurteilt. Die Auswertung erfolgt dabei auf qualitative Weise [Bertsche04] durch ein Maß für die Kritikalität bezüglich der Systemfunktion. Diese wird anhand von größenordnungsmäßigen Bewertungen der Wahrscheinlichkeit der Fehlerursachen und der Schwere der potenziellen Fehlerauswirkungen ermittelt. Andere Methoden hingegen beruhen auf einer quantitativen Grundlage, was eine Berechnung von System-Fehlerwahrscheinlichkeiten anhand der Wahrscheinlichkeiten der möglichen Ursachen erlaubt. Die Fehlerbaumanalyse (englisch: Fault Tree Analysis, FTA) und Zuverlässigkeitsblockdiagramme (englisch: Reliability Block Diagrams, RBD) sind hierzu gebräuchliche Methoden [Bertsche04].

Diese Methoden unterliegen jedoch jeweils spezifischen Vorzügen und Einschränkungen, woraus sich eine jeweils individuell unterschiedliche Qualität des Aufschlusses über die Angemessenheit und eventuelle Kritikalität der vorgesehenen Produktgestaltung ergeben. Während die FMEA nur separate qualitative Kritikalitätseinstufungen jeweils einzelner Ursache-Folge-Beziehungen hervorbringt, ergibt die FTA eine zahlenmäßige Gesamtwahrscheinlichkeit aus den betreffenden Fehlern, die zu einem bestimmten unerwünschten Fehlzustand eines Systems führen können. Diese Bewertung bezieht sich jedoch auf jeweils einen einzelnen Folgezustand. Um die Wahrscheinlichkeit verschiedener unerwünschter System-Fehlzustände zu berechnen, ist es daher notwendig, je einen Fehlerbaum für jeden behandelten System-Fehlzustand zu erarbeiten. Dabei können sich einzelne Ursachen mehrfach in verschiedenen Fehlerbäumen wiederfinden, wobei die probabilistische Auswertung überwiegend ohne Berücksichtigung von statistischen Abhängigkeiten erfolgt. Die probabilistische und die inhaltliche Konsistenz zwischen sich theoretisch ergänzenden Fehlerbäumen eines Systems sind nicht sichergestellt. Auch werden aufgrund der Systematik bei der Erstellung keine Fehlerfolgen aus Ursachen abgeleitet, weswegen keine systematische Erarbeitung der Gesamtheit möglicher Fehlerfolgen durch jeweils einzelne Ursachen erfolgt.

RBD werden im Unterschied zur FTA mit einer gesamtheitlichen Betrachtungsweise erarbeitet. Dazu wird die funktionale Wirkung von Ausfällen von Komponenten dahingehend analy-

siert, ob diese einen Systemausfall bewirken kann. Somit werden dabei keine unterschiedlichen Fehlermöglichkeiten differenziert, sondern nur Funktion und Ausfall.

Die FMEA hingegen liefert ein umfassendes Modell aus allen theoretisch anzunehmenden Ursachen und Konsequenzen in den einzelnen Teilen des Systems. Bei der methodischen Weiterentwicklung der FMEA durch Fehlernetze [VDA-Band4-FMEA:06, DGQ-Band13-11:12] wird zusätzlich ein graphisch formalisiertes Modell, das als Fehlernetz bezeichnet wird, erstellt. Ferner gibt es darauf aufbauende Ansätze, die eine probabilistische Interpretation und Auswertung der Zusammenhänge in Fehlernetzen vorschlagen. Diese sind die Multiple-FMEA [Pickard05], pFMEA [Grunske07] und probFMEA [Kaiser15]. Eine quantitative Auswertung der klassischen FMEA wird in den Konzepten der FMECA [Mil-Std-1629A:80] und FMEDA [Goble99] in beschränktem Umfang umgesetzt.

Wie im Zuge der Arbeit zunächst genauer dargestellt wird, kann mit keiner der bisher üblichen Methoden und der darauf aufgebauten Weiterentwicklungen ein zusammenhängendes, umfassendes und differenziertes kausales Ursache-Wirkungs-Modell für die Gesamtmenge der möglichen Fehler-Folge-Beziehungen eines Systems aufgebaut werden. Als ein vielversprechender Ansatz dafür bietet sich die Verwendung des probabilistische Schemas Bayesscher Netzwerke (BN) nach [Pearl84] an. Es wurde bereits vielfach verwendet, um Fehlermodelle technischer Systeme im Stil der bewährten Methoden darzustellen und zu berechnen, wie beispielweise in [Castillo97, Torres98, Lee99a, Portinale99, Bobbio01]. Ein zusammenhängendes integrales Fehlermodell, im Stil von FMEA-Fehlernetzen oder im Sinne eines umfassenden Gesamt-Zuverlässigkeitsmodells, wurde jedoch noch nicht thematisiert. Hierzu fehlt bislang die analytische Grundlage, um darin verflochtene Ursache-Wirkungsbeziehungen spezifisch zu interpretieren und arithmetisch auszuwerten. Zudem fehlt ein darauf gegründetes methodisches Konzept zur praktischen Umsetzung.

In Anbetracht des verfügbaren Wissensstandes liegt das Ausgangsproblem für die Arbeit nunmehr darin, ein kohärentes probabilistisches Ursache-Folge-Modell für ein System darstellen zu können, das eine differenzierte Zuverlässigkeits- und Fehlzustandsbewertung von Systemen auf probabilistischer Basis erlaubt. Dies ist mit keiner der verfügbaren Methoden entsprechend möglich. Zudem würde ein solches Mehrzustands-Fehlermodell Fortschritt gegenüber den aktuellen arithmetischen Ansätzen und graphisch formalisierten Methoden der Mehrzustands-Zuverlässigkeit darstellen. Eine Randbedingung hinsichtlich Praktikabilität und Akzeptanz ist für solch einen Modellansatz zudem, dass dieses möglichst kompatibel zu den etablierten methodischen Verfahren ist. Optimaler Weise sind keine gänzlich separaten Feh-

lermodelle mittels einer zusätzlichen Methodik anzufertigen, was zudem zur Begrenzung von Arbeitsaufwand beiträgt.

1.2 Zielsetzung

Der Kern dieser Arbeit ist es, probabilistische Netzwerke hinsichtlich deren Nutzbarkeit zur Darstellung und Auswertung integraler Fehlermodelle technischer Systeme zu erschließen. Deren Zweck ist es, die Wahrscheinlichkeit von Fehlerursachen und deren Folgen in einem probabilistisch konsistenten Beziehungsmodell zusammenhängend für Systeme abbilden und berechnen zu können. Das integrale Fehlermodell muss dazu die probabilistischen Beziehungen zwischen Fehlerursachen und Fehlerfolgen zusammenhängend und in konsistenter Weise repräsentieren können. Dazu muss zunächst eine geeignete arithmetische Basis, insbesondere mit Berücksichtigung stochastischer Abhängigkeiten zwischen Fehlzuständen, nachgewiesen werden. Die Prioritäten in dieser Arbeit liegen daher auf der Ausarbeitung benötigter Grundlagen und dem Aufzeigen eines auf dieser Basis darstellbaren methodischen Schemas zur Fehlermodellierung. Zudem sind dessen grundsätzliche Verifikation und Charakterisierung im Hinblick auf die praktische Umsetzbarkeit besonders relevant.

Für den hier thematisierten Ansatz zur Fehlermodellierung besteht das Ziel indes nicht in einer Steigerung der Detailtreue bei der Modellierung physikalischer Gesetzmäßigkeiten beziehungsweise technologischer Phänomene im Rahmen bereits etablierter Methoden. Stattdessen sollen Nützlichkeit und Qualität der Ergebnisse vorrangig dadurch erreicht werden, dass der strukturelle Aufbau das Systemmodell integral und kohärent ist, sodass Wechselwirkungen und Abhängigkeiten darin wiedergegeben werden können. Durch die Randbedingung der probabilistischen Integrität wird ferner berücksichtigt, dass jedes Bauteil und jeder Bauteilverbund gemäß gebräuchlicher Annahmen sich jeweils in genau einem der möglichen exklusiven Fehlerzustände beziehungsweise dem Zustand der Funktionsfähigkeit befinden können. Dieser integrale Ansatz in Verwendung auf gesamte Systeme impliziert insbesondere die Eigenschaften, dass dieser Inkonsistenzen in Form von Betrachtungslücken oder Überbestimmtheit im Fall mehrerer einander inhaltlich überschneidender Teilmodelle eines Systems reduziert. Zudem kann eine kohärente Auswertung des Systems erfolgen, was eine gesamtheitliche Bewertung eines Systems hinsichtlich dessen Zuverlässigkeit, Sicherheit und Qualität ermöglicht.

Die zuvor bereits verwendeten und nicht eindeutig voneinander abgrenzbaren Begriffe „integral“ und „gesamtheitlich“ spielen für die Zielsetzung der Arbeit eine charakterisierende Rolle. Der Begriff „Integral“ bezeichnet dabei den Anspruch auf probabilistische Integrität des logischen und des arithmetischen Modells. Dies bedeutet, dass alle relevanten Beziehungen

zusammen in einem kompakten Modell probabilistisch konsistent und eindeutig enthalten sind. Dabei gilt die Annahme, dass sich jede Teileinheit in einem von mehreren möglichen Zuständen befinden muss. Dazu müssen auch stochastische Abhängigkeiten, wie bedingte Wahrscheinlichkeiten beziehungsweise gegenseitiger Ausschluss verschiedener Zustände, berücksichtigt werden. Durch die Berücksichtigung dieser Randbedingung im Modell wird dessen Güte gegenüber nicht zwingend konsistenten Schemen, wie beispielweise der FTA, erhöht. Durch das Adjektiv „gesamtheitlich" wird im Verständnis dieser Arbeit ausgedrückt, dass zuverlässigkeitsbezogene Zustände unterschiedlicher Art und Auswirkung für eine umsichtige Modellierung in einem kohärenten Fehlermodell dargestellt werden. Dadurch ergibt sich die Möglichkeit, verschiedene Eigenschaften der systemischen Gesamtheit ausgehend von den Eigenschaften der Basisbestandteile beurteilen zu können. Zudem ermöglicht dies die Auswertung unter Berücksichtigung probabilistischer Abhängigkeiten, wie beispielsweise durch den gegenseitigen Ausschluss verschiedener Zustände.

1.3 Herangehensweise und Aufbau der Arbeit

Als Fazit der Problemstellung und der Zielsetzung ergeben sich drei Leitfragen, die als Orientierung für die Umsetzung dienen:

- Wie verhalten sich Fehlerursachen und –folgen und deren Wahrscheinlichkeiten zueinander in einem kohärenten Modell, das die Gesamtheit möglicher Fehlzustände eines Systems beinhaltet?
- Wie lässt sich solch ein kohärentes und integrales Gesamtfehlermodell arithmetisch darstellen und auswerten?
- Wie kann ein probabilistisches Gesamtfehlermodell interpretiert werden und welche technologischen Zusammenhänge lassen sich damit formalisiert wiedergeben?

Die zur Beantwortung dieser Fragestellungen gewählte Herangehensweise spiegelt sich im Aufbau der Arbeit, der aus aufeinander aufbauenden Teilabschnitten besteht, wider (s. Bild 1.1). Vorbereitend wird im zweiten Kapitel der Stand von Wissenschaft und Technik hinsichtlich zutreffender Aspekte der Probabilistik, Zuverlässigkeitstheorie und methodischer Fehlermodellierung dargestellt. In Kapitel drei erfolgt eine Abgrenzung des Ansatzes der Arbeit gegenüber den bisher bestehenden. Ferner werden die wissenschaftliche Methode zur Erschließung der Thematik spezifiziert und Ausgrenzungen einzelner Problemstellungen erörtert. Im vierten Kapitel wird ein Rahmenkonzept zur integralen Fehlermodellierung erarbeitet. Daraus werden nachfolgend rahmengebende Bedingungen, Annahmen und theoretische Hintergründe abgeleitet. Dadurch wird das zugrunde gelegte Verständnis der Problematik

und des Lösungsansatzes systematisch dargestellt. Insbesondere wird das strukturhierarchische Aufbauprinzip von Fehlernetzen diskutiert.

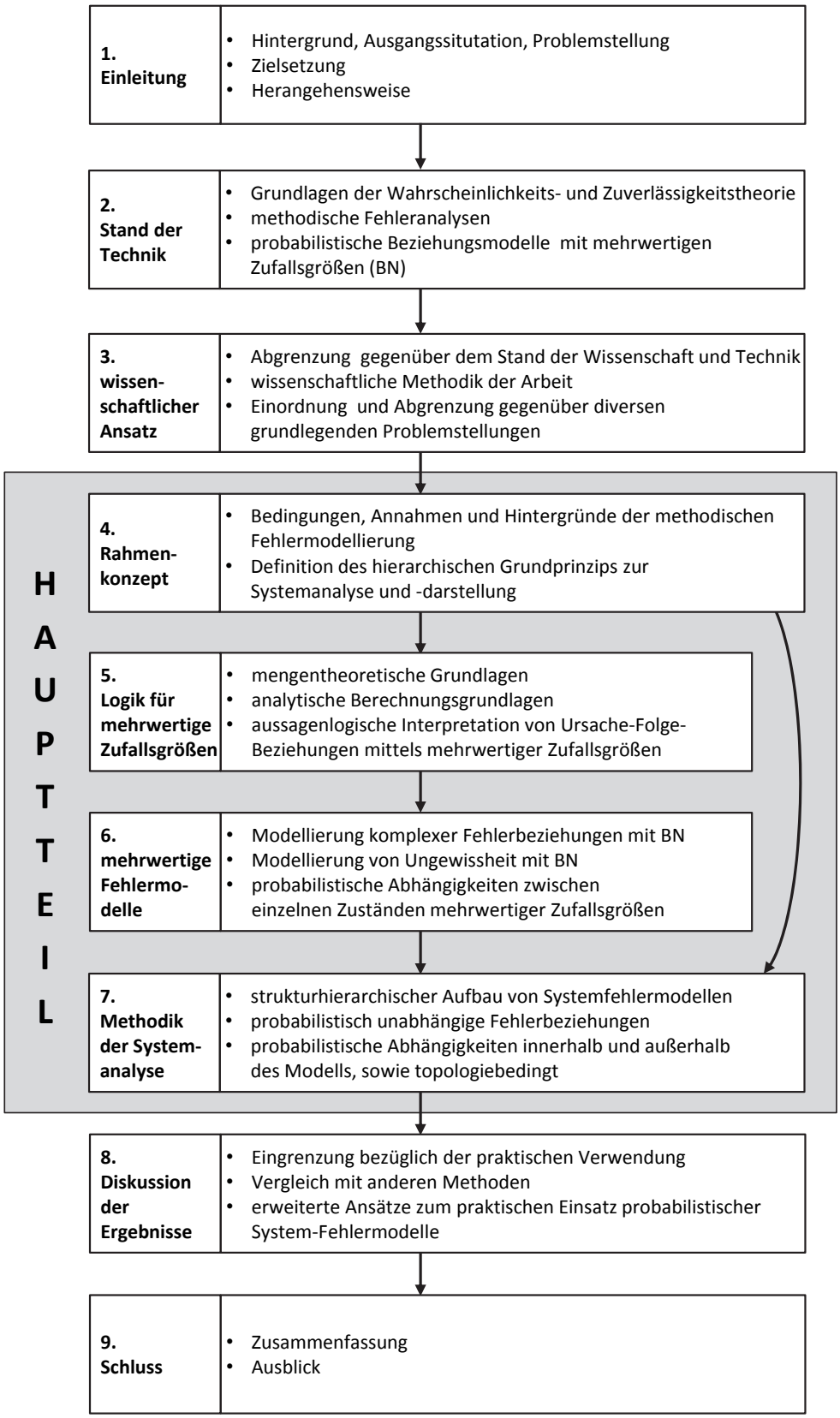


Bild 1.1: schematische Übersicht über Struktur und Inhalte der Arbeit

Kapitel fünf enthält die Herleitung eines integralen arithmetischen Ansatzes zur logisch-probabilistischen Betrachtung von Fehlzuständen auf Basis mehrwertiger diskreter Zufallsgrößen. Dieser ermöglicht aussagenlogische Interpretationen bezüglich der Wahrscheinlichkeiten von Fehlzuständen funktionaler Verbünde sowie deren arithmetische Behandlung. Die in der Herleitung gewonnenen Erkenntnisse dienen nachfolgend zur Charakterisierung und Verifikation des integralen Fehlermodells. Ausgehend von der aussagenlogischen und arithmetischen Systematik des vorangegangenen Kapitels wird in Kapitel sechs die integrale Fehlermodellierung anhand Bayesscher Netzwerke in systemischem Kontext betrachtet. Dazu werden grundsätzliche Eigenschaften, wie stochastische Abhängigkeiten und Ungewissheit im Hinblick auf die Verwendung zur Fehlermodellierung technischer Systeme charakterisiert.

In Kapitel sieben werden die in den beiden vorangegangenen Kapiteln erarbeiteten Grundlagen anwendungsorientiert umgesetzt und diskutiert. Dies erfolgt in Form eines integralen strukturhierarchisch gegliederten System-Fehlermodells, wie es als Bestandteil des Rahmenkonzepts im vierten Kapitel definiert wurde. Dazu werden Ansätze und Schemata zur geeigneten Darstellung typischer Fehlerbeziehungen im Zuge der Fehlermodellierung behandelt. In Kapitel acht werden Ergebnisse der Untersuchungen zusammengetragen und Schlussfolgerungen hinsichtlich der geeigneten Anwendung und aufwandsoptimierten Umsetzung der Methode abgeleitet. Eine abschließende Zusammenfassung und ein Ausblick auf Möglichkeiten zur Weiterentwicklung des Ansatzes sind in Kapitel neun enthalten.

2 Stand der Technik

In der Zuverlässigkeitstheorie und durch methodische Ansätzen zur Fehlermodellierung wird das Verhalten technischer Systeme abgebildet und ausgewertet. Dies jedoch geschieht nicht durch eine unmittelbare Abbildung physikalischer Größen und Gesetzmäßigkeiten in deterministischer Weise. Stattdessen erfolgt eine probabilistische Bemessung durch die Bestimmung der Wahrscheinlichkeiten der Erfüllung bestimmter Eigenschaften und Verhaltensweisen der Systembestandteile. Durch eine formale Systematik wird in Fehlermodellen dabei wiedergegeben, welcher Verhaltenszustand des Systems jeweils dann auftritt, wenn dessen Bestandteile bestimmte fehlerhafte Eigenschaften, beispielsweise bei einem Defekt, aufweisen. Vereinzelt werden auch Ereignisse und besondere Umstände im Betrieb in das Modell einbezogen. Diese Fehlermodelle, die auf logischen Beziehungen beruhen, ermöglichen es letztlich, die Wahrscheinlichkeit des Zutreffens bestimmter Eigenschaften des Systems aus Zusammenfassungen mehrerer möglicher Fehlerursachen zu berechnen.

Nachfolgend werden die wesentlichen Grundlagen und Zusammenhänge dieses probabilistischen Ansatzes diskutiert und darauf aufbauende methodische Ansätze erläutert, die für die nachfolgenden Abschnitte dieser Arbeit relevant sind.

2.1 Grundlagen der Wahrscheinlichkeitstheorie im Rahmen der technischen Zuverlässigkeit

2.1.1 Mengentheorie und -diagramme

Die Mengenlehre ist eine essentielle Grundlage der Wahrscheinlichkeitstheorie und deren Verfahren. Die wissenschaftliche Begründung wird Georg Cantor zugerechnet: „Unter einer ‚Menge' verstehen wir jede Zusammenfassung M von bestimmten wohlunterschiedenen Objekten m unserer Anschauung oder unseres Denkens (welche die ‚Elemente' von M genannt werden) zu einem Ganzen." [Cantor1895]. Cantor definiert dazu ein Axiomensystem, das unter anderem die Konzepte der Mächtigkeit einer Menge auf Basis der Anzahl der in ihr enthaltenen Elemente sowie der Teilmenge, Mengenschnitte und Mengenvereinigungen enthält. Außerdem werden die Addition und Multiplikation der Mächtigkeiten zweier Mengen definiert, sowie die Gesetzmäßigkeiten der Kommutativität, Assoziativität und Distributivität aufgezeigt.

Mengenbeziehungen können in Mengendiagrammen veranschaulicht werden. Dafür gibt es zwei verbreitete Darstellungsprinzipien, die durch Euler [Euler1761] beziehungsweise Venn [Venn1880] definiert wurden. Weise [Lange1712, Hamilton1863] definierte ein zu Eulerdia-

grammen quasi identisches Verfahren. In Mengendiagrammen werden Mengen als geschlossene geometrische Formen dargestellt. Durch die Anordnung mehrerer solcher Mengen repräsentierender Elemente werden deren inhaltliche Beziehungen zueinander symbolisiert. Beispielsweise kennzeichnet die Überschneidung von Kreisen oder Ellipsen gemeinsame Teilmengen. Die dadurch definierte Schnittmenge enthält Elemente, die beiden Hauptmengen gleichermaßen angehören.

In Euler-Diagrammen werden Mengen durch Formen unterschiedlicher Größe dargestellt, die sich entweder teilweise überschneiden (Schnittmenge), gänzlich in einer anderen enthalten sind oder aber keine gemeinsame Überschneidung haben (s. Bild 2.1 links). Eulerdiagramme sind jedoch nicht in jedem Fall eindeutig [Venn1880] und können daher nicht in beliebigem Kontext zur universellen Beweisführung verwendet werden.

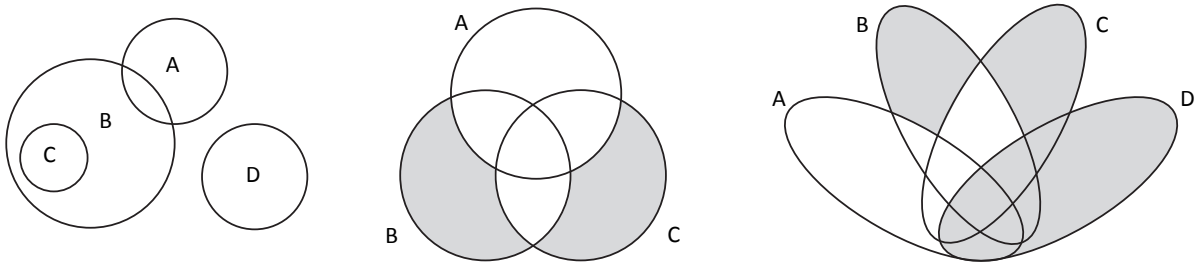


Bild 2.1: zufällige Beispiele für Mengendiagramme nach [Euler1761] (links) beziehungsweise nach [Venn1880] für drei (mittig) und vier Mengen (rechts)

Zudem schlug Venn ein nach eigener Einschätzung von Eulerdiagrammen grundsätzlich verschiedenes Verfahren zur graphischen Repräsentation von Mengen vor, welches hingegen in [Chow97] als eine Unterklasse von Eulerdiagrammen eingestuft wird. Dazu werden alle in einem Aussagenkontext miteinander in Bezug stehenden Mengen einander in allen theoretisch möglichen Konstellationen überlagert dargestellt (s. Bild 2.1 mittig). So werden darin grundsätzlich alle möglichen Kombinationen von Schnitten der Grundmengen repräsentiert, zusammen mit der diese umgebenden Fläche. Die darzustellende Aussage wird gekennzeichnet, indem Schnittmengen durch Ausstreichen, beispielsweise durch Einschwärzen solcher Flächen ausgegrenzt werden, soweit die betreffende Aussage für diese nicht zutrifft. Venn-Diagramme lassen sich für bis zu vier Mengen mit elementaren geometrischen Formen bilden (s. Bild 2.1 rechts). Größere Anzahlen können jedoch nicht mehr trivial konstruiert werden [Carroll05].

Auch gegenüber Venn-Diagrammen bestehen Vorbehalte [Couturat1914]. Deren Verwendung als universelle Methode logischen Folgerns und Argumentierens ist daher beschränkt,

da mit Ihnen keine Methodik zur systematischen Analyse und Ableitung von Folgerungen einhergeht. Es ist anzunehmen, dass hierin der Grund liegt, weswegen in wissenschaftlichen Arbeiten zu aussagenlogischen Problemstellungen diese graphischen Methoden bislang in eher begrenztem Maß und vorrangig zur Illustration verwendet werden [Shin94]. Dies wiederum erweist sich als Bezugspunkt wissenschaftlicher Aktivitäten der jüngeren Vergangenheit. In [Fitzpatrick75] wurden eine Erweiterung von Venn-Diagrammen und eine Entscheidungsprozedur als ergänzende Methode vorgeschlagen. In einer Reihe weiterer Arbeiten wurden weitergehenden Möglichkeiten zur Ausweitung und Nutzung der Mengendiagramme zur Repräsentation und Ableitung formaler Schlussfolgerung [Shin91, Shin94, Hammer96, Swoboda97, Hammer98, Gurr98, Swoboda02] behandelt. Unter anderem wurde in [Shin94] ein formales System auf Basis von Venn-Diagrammen vorgestellt, das das Argumentieren und Schlussfolgern anhand von erweiterten Mengendiagrammen erlaubt. In [Hammer96] wird ein Ansatz zur Untersuchung eines logischen Systems mit Diagrammen anstelle von Formeln diskutiert. Doch auch diese sind nicht fundamental ausdefiniert hinsichtlich aller graphischen Eigenschaften und deren Bedeutung, sondern nur aufgrund von abstrahierter Betrachtung und innerhalb bestimmter mengentheoretischer Randbedingungen [Gurr98]. Einen umfassenden Überblick über die bis dahin verfügbaren wissenschaftlichen Arbeiten diesbezüglich findet sich in [Stapleton05]. Auch nachfolgend wurde das Thema fortgesetzt behandelt. In [Swoboda05] wird eine als „Euler/Venn-Diagramme" bezeichnete Mischform nebst zugehöriger Systematik für logisches Schlussfolgern innerhalb einer Logik erster Ordnung vorgeschlagen.

2.1.2 Klassische Logik

Nach Jaynes ist die „[…] Wahrscheinlichkeitstheorie, wie sie von Laplace begründet wurde, eine Generalisierung Aristotelischer Logik, die sich in dem Spezialfall, dass unsere Hypothesen entweder wahr oder falsch sind, zu einer deduktiven Logik reduziert." (übersetzt aus dem Englischen) [Bretthorst14]. Deduktiv bedeutet dabei, dass Schlussfolgerungen über Wahrheit oder Unwahrheit eines Sachverhalts anhand einer Theorie oder Gesetzmäßigkeit getroffen werden [Jevons1888]. Im Unterschied hierzu wird bei der Induktion aus einzelnen Beobachtungen auf eine Theorie oder Gesetzmäßigkeit zurückgeschlossen. In der klassischen Logik [Frege1879, Arnauld72] kann eine Aussage entweder zutreffend oder nicht zutreffend sein. Somit gibt es zwei Wahrheitswerte {‚$\boldsymbol{wahr}$'} oder {‚$\boldsymbol{falsch}$'}, was unter anderem als Zweiwertigkeit und Bivalenz bezeichnet wird. In der internationalen Zuverlässigkeitsliteratur werden hierfür auch die Adjektive binär und dual synonymisch verwendet (übersetzt aus dem Englischen „binary" beziehungsweise „dual").

Ein weiterer Grundsatz klassischer Logik ist das Extensionalitätsprinzip oder auch Kompositionalitätsprinzip. Nach diesem kann der Wahrheitswert einer zusammengesetzten Aussage von den Wahrheitswerten einzelner Aussagen abgeleitet werden. Dabei spielt auch die Weise wie sich diese zusammensetzen eine Rolle. In anderen Worten ausgedrückt handelt es sich dabei um das Prinzip, Folgerungen aus Aussagenkombinationen mittels Regeln der Form „wenn… dann…" abzuleiten wie „Wenn A gilt und zugleich B gilt, dann gilt folglich C ".

Es gibt diverse Ansätze, die klassische Logik über die Zweiwertigkeit hinaus zu erweitern. Nach [Jaynes03] sind jedoch alle aktuellen Entwicklungen solcher mehrwertigen Logiken beispielsweise in Quantentheorie, unscharfer Mengentheorie (aus dem Englischen: „Fuzzy-Set-Theory") und künstlicher Intelligenz inkonsistent beziehungsweise lieferten diese keine nützlichen Antworten über bereits mit zweiwertiger Logik zu lösende Probleme hinaus. So lehnt Jaynes den Ansatz einer mehrwertigen Logik zwar nicht prinzipiell ab, dagegen jedoch die bis dato vorgeschlagenen Modelle.

2.1.3 Logikkalkül

Boole [Boole1847] entwickelte die Grundlage eines zweiwertigen Logikkalküls, für das im Zuge nachfolgender Weiterentwicklungen erstmals durch Peano [Peano1888] eine zweiwertige Algebra definiert wurde, die seither der sogenannten Booleschen Algebra zugrunde liegt. Diese weist die Form auf, nach der sich die gebräuchliche Verwendung des Logikkalküls in der technischen Zuverlässigkeit richtet. So können logische Aussagen und in Mengen zusammengefasste Gruppen von Aussagen als Größen in Termen dargestellt und ausgewertet werden. Dies ist die Grundlage für eine algebraische Auffassung von Sätzen der Art „System X fällt aus, wenn Teilsystem A oder B oder beide ausfallen".

Für die Boolesche Algebra wurden logische Verknüpfungen als essentielle Operatoren zur algebraischen Behandlung logischer Aussagen festgelegt. Auf Basis der Wahrheitswerte zweier Aussagen A und B definieren diese logischen Funktionen den Wahrheitswert einer von diesen abhängigen Größe X:

- UND-Operator (Konjunktion): $X = A \cap B$

  „X *ist wahr, wenn* A *und* B *wahr sind.*"

- ODER-Operator (Disjunktion, inklusiv): $X = A \cup B,$

  „X *ist wahr, wenn* A, B *oder beide wahr sind.*"

- NICHT-Operator (Negation): $X = -A,$

„X ist wahr, wenn A nicht wahr ist."

Zudem existiert eine alternative Form der exklusiven Disjunktion, die jedoch nicht in der Axiomatik von Peano verwendet wurde:

- XODER-Operator (Disjunktion, Exklusiv): $X = A \underline{\cup} B,$

„X ist wahr, wenn entweder nur A oder nur B wahr ist."

Das in [Peano1888] dargestellte Axiomensystem umfasst mehrere Gesetze, die zur Umformung und Auswertung logischer Terme verwendet werden (s. Tabelle 2.1).

Tabelle 2.1: Axiomensystem nach [Peano1888]

Kommutativgesetze	(1)	$AB = BA$	(1′)	$A \cup B = B \cup A$
Assoziativgesetze	(2)	$A(BC) = AB$	(2′)	$A \cup (B \cup C) = A \cup B \cup C$
Idempotenzgesetze	(3)	$AA = A$	(3′)	$A \cup A = A$
Distributivgesetze	(4)	$A(B \cup C) = AB \cup AC$	(4′)	$A \cup BC = (A \cup B)(A \cup C)$
Neutralitätsgesetze	(5)	$A \cap \Omega = A$	(5′)	$A \cup \{\} = A$
Extremalgesetze	(6)	$A \cap \{\} = \{\}$	(6′)	$A \cup \Omega = \Omega$
Involutionsgesetz	(7)	$-(-A) = A$		
De Morgansche Gesetze	(8)	$-(AB) = (-A) \cup (-B)$	(8′)	$-(A \cup B) = (-A) \cap (-B)$
Komplementärgesetze	(9)	$A \cap -A = \{\}$	(9′)	$A \cup -A = \Omega$
Dualitätsgesetze	(10)	$-\{\} = \Omega$	(10′)	$-\Omega = \{\}$
Absorptionsgesetze	(11)	$A \cup AB = A$	(11′)	$A(A \cup B) = A$

Anhand der Axiome von Peano können Terme aus mehreren Operationen zur Vereinfachung umgeformt werden, was in der Zuverlässigkeitstheorie unter anderem als „boolean simplification" [Watson62, DeLong70] bezeichnet wird. Dies spielt bei der Auswertung von Fehlermodellen eine wesentliche Rolle, wofür üblicherweise als Minimalschnitte bezeichnete Teilterme (aus dem Englischen „Minimal Cut Sets" [Vesely81]) ermittelt werden. Diese sind die minimalen Schnittmengen, für die die resultierende Aussage eines Terms wahr ist, beispielsweise der Systemausfall im Kontext von Fehlermodellen. In diesem Zustand bestehen die Gleichungen aus Teiltermen die disjunktiv (ODER) miteinander verbunden sind. Die Teilterme selbst bestehen aus einer einzelnen Aussage oder einer Konjunktion (UND-Verknüpfung) mehrerer Einzelaussagen, beispielsweise:

$$X = (A \cap B) \cup (C \cap D) \tag{2.01}$$

So ist es in diesem Zusammenhang typischerweise das Ziel, logische Terme erstellter Fehlermodelle in eine als disjunktive Normalform bezeichnete Gestalt zu transformieren:

$$\cup_i \cap_j (-) x_{ij} \tag{2.02}$$

Die darin enthaltenen einzelnen konjunktiven Teilterme werden als Minterme oder Elementarkonjunktion bezeichnet. Nachfolgend werden diese in dieser Arbeit auch als elementare Schnittmengen bezeichnet, um deren Bezug auf die mengentheoretische Betrachtung der Kombinationen von Komponentenzuständen zu verdeutlichen. Trifft die in einem solchen Minterm beschriebene Kombination von Aussagen zu, so ist die Aussage X als Ergebnis des Terms ebenfalls zutreffend. Sei beispielsweise:

$$X = (-A \cap B) \cup (C \cap D) \tag{2.03}$$

Nimmt man exemplarisch für A den Wert {‚$falsch$'} und für B {‚$wahr$'} an, gilt

$$-\mathrm{A}(\text{'falsch'}) = \{\text{'wahr'}\} \quad \Rightarrow \quad (-\mathrm{A} \cap \mathrm{B}) = \{\text{'wahr'}\}$$

Dadurch ist X nach Gleichung (2.03) für beliebige Werte für C und D stets wahr, da der erste der beiden Minterme zutrifft. Analog würde dies für den zweiten Minterm des Beispiels gelten, ebenso wie für beliebig umfassende logische Ausdrücke in der disjunktiven Normalform. Daher eignet sich diese Form gut zur Auswertung komplexer logischer Ausdrücke.

2.1.3 Probabilistik

Die Grundlage der klassischen Wahrscheinlichkeitstheorie, die auch der Zuverlässigkeitstechnik zugrunde liegt, geht maßgeblich auf Laplace [Laplace1812] zurück. Nach der frequentistischen Auffassung entspricht die Wahrscheinlichkeit eines Ereignisses eines sogenannten Laplaceschen Zufallsexperiments dem Verhältnis zwischen den für eine Aussage A zutreffenden und allen aufgetretenen Ergebnissen.

$$P(A) = \frac{P(A = \{'wahr'\})}{P(A = \{'wahr', 'falsch'\})} \tag{2.04}$$

Zur Bestimmung der Wahrscheinlichkeit muss ein Zufallsexperiment, wie beispielsweise das Werfen eines idealen Würfels, theoretisch unendlich oft erfolgen, beziehungsweise real mit einer ausreichenden Anzahl von Wiederholungen unter identischen Bedingungen.

In der hiervon unterschiedlichen subjektivistischen Wahrscheinlichkeitsauffassung, die auf Bayes [Bayes1763] zurückgeht, fasst man Wahrscheinlichkeit als Grad der Überzeugung

(englisch: „degree of belief“) auf. In der Form kann auch zusätzliches Wissen in Schätzungen der Wahrscheinlichkeit berücksichtigt werden, beispielsweise durch verschiedene Randbedingungen und auf Basis von Erfahrung. Nach [Pearl00] beruhen die Auffassungen von Wahrscheinlichkeit im subjektivistischen Sinn als Überzeugung sowie im frequentistischen Sinn als Häufigkeit wiederum auf derselben Grundlage, weswegen diese zueinander nicht prinzipiell inkompatibel sind. Ähnlich ist es nach Jaynes Auffassung nicht sinnvoll, zu entscheiden, ob entweder bayessche oder frequentistische Verfahren einen gültigen Ansatz darstellen. Da beide nicht universell verwendbar seien, postuliert er, die „Wahrscheinlichkeit als erweiterte Logik“ [Jaynes03] (übersetzt aus dem Englischen) auffassen zu können, was beide Konzepte einschließt.

Durch das Kolmogorowsche Axiomensystem [Kolmogorow33] wird die in der heutigen Systemzuverlässigkeit gebräuchliche probabilistische Interpretation der Mengentheorie ermöglicht. Dies wiederum stellt die Grundlage zur Anwendung der Logik und deren Kalkül in der Wahrscheinlichkeitstheorie dar. Demnach wird Mengen ein Wahrscheinlichkeitsmaß zugeordnet und ein Gesamt-Ergebnisraum $\boldsymbol{\Omega}$ mit der totalen Wahrscheinlichkeit $\boldsymbol{P(\Omega) = 1}$ definiert. Die darin enthaltenen Ereignismengen und zugeordnete Wahrscheinlichkeiten können mathematisch interpretiert und behandelt werden. Das Zutreffen mehrerer Aussagen, also deren Schnittmenge, errechnet sich aus dem allgemeinen Multiplikationssatz, der auf dem Konzept der bedingten Wahrscheinlichkeit beruht. So bezeichnet $\boldsymbol{P(B|A)}$ die Wahrscheinlichkeit, mit der $\boldsymbol{B}$ gilt, unter der Bedingung, dass $\boldsymbol{A}$ bereits eingetreten ist. Umgekehrt gilt die Wahrscheinlichkeit $\boldsymbol{P(A|B)}$ für das Eintreten von $\boldsymbol{A}$, wenn auch $\boldsymbol{B}$ vorliegt. Dies drückt sich im Multiplikationssatz für zwei Zufallsgrößen $\boldsymbol{A}$ und $\boldsymbol{B}$ aus (Bayessches Theorem) [Bayes1763]:

$$P(A \cap B) = P(B|A)P(A) = P(A|B)P(B) \tag{2.05}$$

Treten $\boldsymbol{A}$ und $\boldsymbol{B}$ zufällig und unabhängig voneinander auf, ist $\boldsymbol{P(B|A) = P(B)}$ beziehungsweise $\boldsymbol{P(A|B) = P(A)}$, sodass gilt [Feller50, Pfeiffer65]:

$$P(A \cap B) = P(A)P(B) \tag{2.06}$$

Für die Disjunktion der unabhängigen Größen ist:

$$P(A \cup B) = P(A) + P(B) - P(A)P(B), \quad \text{für } A \parallel B \tag{2.07}$$

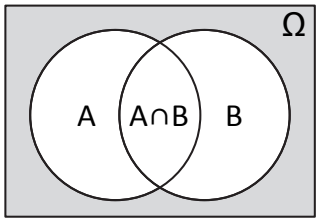


Bild 2.2: Mengendiagramm eines Schnitts zweier unabhängiger Ereignismengen A und B

Für die exklusive Disjunktion wird der Wahrscheinlichkeitswert der gemeinsamen Schnittmenge zusätzlich subtrahiert, sodass:

$$P(A \underline{\cup} B) = P(A) + P(B) - 2 \cdot P(A)P(B), \quad \text{für } A \parallel B \tag{2.08}$$

Die Gesamtwahrscheinlichkeit zweier sich gegenseitig ausschließender Ereignisse A und B hingegen ist deren arithmetische Summe, da sie keine gemeinsame Schnittmenge bilden:

$$P(A \cup B) = P(A) + P(B), \quad \text{für } A \perp B \tag{2.09}$$

Für mehrere Größen A, B, C, … lautet der allgemeine Multiplikationssatz kombinierter Wahrscheinlichkeiten [Feller50, Pfeiffer65, Vesely81]:

$$P(A \cap B \cap C \cap \dots) = P(A)\, P(B|A)\, P(C|A \cap B)\, P(\dots|A \cap B \cap C)\ \dots \tag{2.10}$$

Sind A und B jeweils probabilistisch abhängig von einer weiteren Größe C, gilt ferner für das allgemeine Bayes-Theorem [Russell95]:

$$P(A|B,C) = \frac{P(B|A,C)P(A|C)}{P(B|C)} \tag{2.11}$$

In [Pfeiffer65, Vesely81] wird im Kontext der technischen Zuverlässigkeit dargestellt, wie probabilistische Ereignisse auf Grundlage der Kolmogorowschen Wahrscheinlichkeitsdefinition mengentheoretisch interpretiert und aussagenlogisch behandelt werden können. Unter anderem wird dargelegt, dass Mengen A in Partitionen i unterteilt werden können (s. Bild 2.3 links), deren einzelnen Wahrscheinlichkeiten $P(a_i)$ zur Gesamtwahrscheinlichkeit $P(A)$ addieren, da diese gegenseitig exklusiv sind und sich daher nicht überschneiden:

$$P(A) = \sum_{i \in J} P(a_i)\,, \qquad mit\ \ a = \{a_i : i \in J\} \tag{2.12}$$

Bild 2.3: Mengendiagramm eines Schnitts von Sektionen des Gesamtraums S (sicheres Ereignis) und dem Ereignis A (links) nach [Pfeiffer65] sowie (rechts) in Partitionen A_i unterteilter Ergebnisraum Ω im Schnitt mit einer Ereignismenge B nach [Vesely81]

2.2 Theorie der Zuverlässigkeit technischer Systeme

Die probabilistischen Grundlagen der Zuverlässigkeit von Systemen wurden im Laufe des vergangenen Jahrhunderts, unter anderem durch [Fry28, Feller50, Carhart53, Bazowsky61, Barlow65, Chorafas60] erschlossen. Eine zusammenfassende Darstellung der anfänglichen Entwicklung dieser Wissenschaftsdisziplin ist in [Barlow84] zu finden. Diese Grundlagen bilden das Fundament der heutigen Zuverlässigkeitstechnik, die seither ein breites akademisches und praktisches Betätigungsfeld darstellt. Dies zeigt sich anhand zahlreicher Grundlagenwerke, wie unter anderem [DIN 40041:90, Barlow96, Rakowsky01, DGQ-Band17-10:02, Bertsche04, Rausand04, VDA-Band3:04, VDI4001:06, Bertsche09, Stapelberg09, Smith11, Birolini14].

Grundsätzlich handelt es sich bei Bauteilausfällen um deterministische Vorgänge [Chorafas60], die wie das Zufallsexperiment des Würfelns durch physikalische Gegebenheiten bedingt sind [Jaynes03]. Jedoch ist die deterministische Berechnung von Ausfallzeitpunkten und deren Streuung für technische Systeme zumindest nicht praktikabel, da hierfür exakte Berechnungsmodelle mit Berücksichtigung aller Einflussgrößen nötig wären. Zudem sind alle Werte zu bestimmen, die einen Einfluss auf Eigenschaftsveränderungen haben. Zu berücksichtigen sind dabei unter anderem auch Zusammenhänge und Einflüsse, wie beispielsweise die Fehlerphysik auf mikroskopischer Ebene, fertigungsbedingte Streuung von Bauteileigenschaften, alle Einflussgrößen im Inneren des Systems und dessen Umgebung, funktionale Wechselwirkungen sowie spezifische Nutzungs- und Beanspruchungshistorien individueller Systeme. Als Alternative werden daher stochastische Konzepte zur Bemessung der Zuverlässigkeit angewendet, um in verallgemeinerter Form auf die Wahrscheinlichkeit des Aufkommens fehlerhafter Komponenteneigenschaften anhand von Referenzdaten zurückschließen zu können. Eine der vermutlich ersten probabilistische Definitionen der Zuverlässigkeit technischer Systeme wurde in dem Projekt RAND festgehalten:

„Die Zuverlässigkeit einer gegebenen Komponente oder eines gegebenen Systems ist die Wahrscheinlichkeit, dass es dessen erforderliche Funktion unter gegebenen Bedingungen für einen festgelegten Zeitraum erfüllt." [Carhart53] (übersetzt aus dem Englischen).

Definitionen der Zuverlässigkeit in zeitgenössischen Werken [Barlow98, MIL-HDBK338B:98, NASA-STD-8729.1:98, Bertsche04, VDI4001:06, Birolini14] entsprechen dieser inhaltlich und sinngemäß zumindest weitgehend. Einzelne beziehen die Zuverlässigkeit auf das Kriterium des Ausfalls im engeren Sinn wie beispielsweise in [Bertsche04]:

„Zuverlässigkeit ist die Wahrscheinlichkeit dafür, dass ein Produkt während einer definierten Zeitdauer unter gegebenen Funktions- und Umgebungsbedingungen nicht ausfällt."

In [Rakowsky01] wird betont, dass die Zuverlässigkeit an sich keine Wahrscheinlichkeit impliziert. Die Wahrscheinlichkeit ist dagegen eine Maßgröße, die zur Darstellung der Eigenschaft der Zuverlässigkeit genutzt werden kann. Analog dazu ist die Zuverlässigkeit beziehungsweise Funktionszuverlässigkeit in [VDI4003:07, IEC60050:192:15 (Referenz: 192-01-24)] als eine Fähigkeit einer Einheit definiert, eine geforderte Funktion unter gegebenen Bedingungen für ein gegebenes Zeitintervall zu erfüllen. Dagegen wird Zuverlässigkeit im Sinne einer Maßgröße nach [IEC60050:192:15 (Referenz: 192-05-05)] als eine Wahrscheinlichkeit aufgefasst.

Bei einer probabilistischen Abschätzung der Systemzuverlässigkeit $R(t)$ geht es demnach prinzipiell darum, eine probabilistische Bewertung der Funktionsfähigkeit eines Systems zu erlangen. So gilt grundsätzlich für die Zuverlässigkeit $R(t)$ zum Zeitpunkt t:

$$R(t) = f(t) \quad , \quad P('X \text{ ist in t nicht funktionsfähig'}) \tag{2.13}$$

Nach der verbreiteten Auffassung der technischen Zuverlässigkeit gilt der komplementäre Zusammenhang zwischen spezifizierter Funktion und den dieser entgegenstehenden Fehlern. So grenzt die Auffassung der Zuverlässigkeit zugleich den Zustand eines fehlerhaften Verhaltens ab, aufgrund dessen die Eigenschaft der Zuverlässigkeit nicht erfüllt wird. Für die Fehlerwahrscheinlichkeit $F(t)$ gilt damit:

$$F(t) = 1 - R(t) \quad , \quad P('X \text{ ist in t nicht funktionsfähig'}) \tag{2.14}$$

Dabei beruht die Fehlerwahrscheinlichkeit eines Systems auf den Wahrscheinlichkeiten der Bauteile, dass diese durch einen Defekt oder eine Veränderung deren Funktion nicht mehr angemessen erfüllen, was ein fehlerhaftes Systemverhalten verursacht [Knight55]. Nach

[Bromberg53, Carhart53, Moore56] kann die Zuverlässigkeit von Baugruppen und Systemen nach dem Multiplikationssatz aus den unabhängigen Zuverlässigkeitswerten von n Bauteilen in Reihenschaltung beziehungsweise Parallelschaltung n redundanter Komponenten ermittelt werden. Nach [Bromberg53] ist dies:

$$R_{total} = R_1 R_2 \ \dots R_i \ \dots R_n \quad (Reihenschaltung) \tag{2.15}$$

$$R_{total} = 1 - (1 - R_i)^n \quad (Parallelschaltung, redundant) \tag{2.16}$$

Als Kennwert der Zuverlässigkeit wird oft die Ausfallrate $\lambda(t)$ genutzt, die definiert ist durch:

$$\lambda(t) = -\frac{\frac{dR(t)}{dt}}{R(t)} \tag{2.17}$$

Für die Ausfallwahrscheinlichkeit $F(t)$ gilt dabei:

$$F(t) = 1 - R(t) = 1 - e^{\int_0^t \lambda(t)dt} \tag{2.18}$$

Diese Ausfallwahrscheinlichkeit als zeitabhängige Funktion hängt vom individuellen Bauteil und Einwirkungen auf dieses ab. Durch diese ist die Ausfallrate allgemein zeitabhängig. Als Näherung werden vielfach konstante Ausfallraten angenommen und zur Zuverlässigkeitsbewertung genutzt [Bazowsky61]. Dies vereinfacht die mathematische Behandlung der Terme von Fehlermodellen mitunter erheblich [Vesely81]. Dies jedoch trifft nur unter entsprechenden Randannahmen und Einschränkungen sowie günstigstenfalls in guter Näherung zu. Die Verwendung dieser Vereinfachung ist nicht für alle Arten von Bauteilen und nicht für alle Bewertungsaufgaben gleichermaßen zutreffend beziehungsweise korrekt [Watson62, Eckberg63, Bowles02].

2.3 Klassische Methoden zur Fehlermodellierung und darauf aufbauende Ansätze

Die Methoden zur Fehlermodellierung werden anhand deren probabilistischer Eigenschaften in qualitative und quantitative unterteilt [Bertsche04]. Im Unterschied zu qualitativen Methoden werden in quantitativen Methoden probabilistische Gesetzmäßigkeiten und ein jeweils spezifischer Modellierungsformalismus genutzt, um anhand dessen die Wahrscheinlichkeiten des Eintretens zu bewertender Eigenschaften berechnen zu können. Dies sind typischerweise die Zustands- und Ereigniswahrscheinlichkeit von Fehlern im System, wobei auch Ansätze

zur Modellierung und Berechnung physikalischer Größen auf der Grundlage von Fehlerwahrscheinlichkeiten entwickelt wurden, wie unter anderem in [Misra08, Natvig11] erläutert wird.

Die nicht allgemein definierten Begriffe eines Fehlermodells und der Fehlermodellierung werden nachfolgend in dem Verständnis genutzt, dass ein Fehlermodell ein abstrahiertes und formalisiertes Abbild von Wirkweisen und Wirkbeziehungen fehlerhafter Eigenschaften und Zustände in technischen Systemen darstellt.

2.3.1 Quantitative Methoden

In quantitativen Methoden zur Fehlermodellierung werden die Wahrscheinlichkeits- und Zuverlässigkeitstheorie genutzt, um die Wahrscheinlichkeit von Fehlern eines Systems zu berechnen [Bertsche04]. Dazu werden logische Modelle gebildet, die Aussagen darüber graphisch symbolisieren, welche Zustände des Systems vorliegen, wenn jeweils solche Fehlzustände von Komponenten eintreten, die diese verursachen. Anhand dieser Beziehungen kann mit dem probabilistischen Ansatz des Logikkalküls die Wahrscheinlichkeit eines Systemzustands aus den Wahrscheinlichkeiten der dazu führenden Ursachen berechnet werden. Dies geschieht auf die in [Bromberg53] aufgezeigte Weise. Diese beruht auf der Auswertung der Fehlerwahrscheinlichkeiten anhand der Einordnung der funktionalen Abhängigkeiten im Sinne serieller und paralleler Anordnungen. Auf diesem Ansatz beruhen die Methoden der Fehlzustandsbaumanalyse (englisch: Fault Tree Analysis, FTA) [Watson62, Eckberg63, DeLong70, Vesely81, Vesely02, VDA-Band4:03, DIN-IEC-61025:07] und Zuverlässigkeitsblockdiagramm (englisch: Reliability Block Diagram, RBD) [DIN-EN-61087:06]. Die Entwicklung der RBD-Methode zugrundeliegenden Ansatzes lässt sich in [Bromberg53, Carhart53, Moore56, Chorafas60, Bazovsky61] nachvollziehen. Im Folgenden werden die englischen Kurzbezeichnungen der FTA und RBD vereinfachend und in Analogie zur internationalen Fachliteratur weiter verwendet.

Für die FTA ist das Fehlermodell als ein Baumgraph aus Symbolen logischer Operatoren definiert. Mit diesen werden die Ursachen so verbunden dargestellt, dass dadurch gekennzeichnet wird, welche Ursachen jeweils alternativ (ODER, Disjunktion) beziehungsweise in Kombination (UND, Konjunktion) zu der Folge führen, wie dies in Bild 2.4 links beispielhaft dargestellt ist. So können nachfolgend die Wahrscheinlichkeiten möglicher ursächlicher Fehler und Fehlerkombinationen mittels logischer Operationen miteinander verrechnet werden. Daraus ergibt sich die gesamte Wahrscheinlichkeit des Vorkommens einer jeweils spezifischen Folge auf der systemisch höchsten Ebene, dem sogenannten Hauptereignis (englisch:

Top-Event). Es wurden zahlreiche auf die ursprüngliche FTA-Methode und deren Weiterentwicklung bezogene Arbeiten veröffentlicht, was sich anhand der Zusammenfassungen in [Lee85, Kuznetsov94, Ericson99, Ruijters15] im Überblick nachvollziehen lässt.

Für RBD ist ein Netzwerkschema vorgegeben, das Komponenten des Systems als Blöcke in deren funktionaler Verkettung darstellt. Darin reihen sich die Blöcke aneinander an, die für die erfolgreiche Funktion zusammenwirken müssen. Weist ein einzelner Teil dieser Kette, also eine Komponente, einen Fehler auf, wird dies als Fehler für das System eingestuft. Dies entspricht einer logischen ODER-Beziehung. Redundante Komponenten, die sich bei einem Ausfall gegenseitig funktional substituieren können, werden als nebeneinander stehende Blöcke parallel im Netzwerk dargestellt (s. Bild 2.4 rechts). Dies entspricht einer UND-Operation, was logisch ausdrückt, dass das Gesamtsystem dann ausfällt, wenn alle der parallel angeordneten Komponenten nicht funktionsfähig sind.

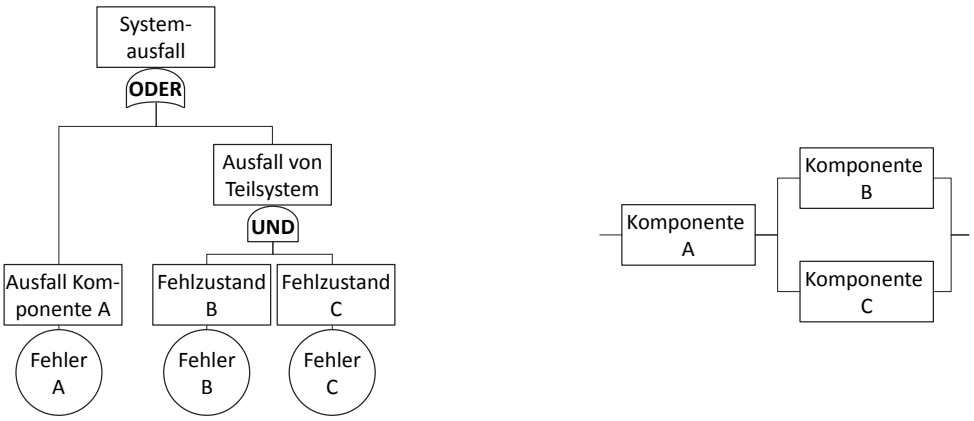


Bild 2.4: graphische Repräsentation von Fehlermodellen in FTA (links) und RBD (rechts)

Bild 2.4 zeigt links einen Fehlerbaum (FT) und rechts ein RBD jeweils für einen Systemausfall S, der eintritt, wenn die Komponente A ausgefallen ist oder zugleich beide Komponenten B und C. Aus beiden Graphen lässt sich anhand deren Symbolik beziehungsweise Topologie der logische Term

$$S = A \cup (B \cap C) \tag{2.19}$$

ableiten. Dies ermöglicht die Berechnung der Wahrscheinlichkeit des Systemausfalls $F(S)$, unter der Annahme, dass A, B und C voneinander unabhängig sind und sich nicht gegenseitig ausschließen:

$$P(S) = P(A) + P(B \cap C) - P(A)\,P(B \cap C) = P(A) + P(B)\,P(C) - P(A)\,P(B)\,P(C) \tag{2.20}$$

Im thematischen Umfeld dieser Arbeit sind einzelne spezifische Erweiterungen der FTA-Methodik nennenswert. In der sogenannten Dynamic FTA [Dugan92] wird die klassische FTA-Methodik um logischen Gatter erweitert, in welchen funktionale Bedingungen und zeitliche Abfolgen berücksichtigt werden können. Das Grundkonzept, nach dem jeweils ein Fehlerbaum für jeden Fehlzustand des Systems, also je Hauptereignis des Fehlerbaums, aufzubauen ist, gilt unverändert. In [Kaiser03] wurde ein als Component Fault Tree (CFT) bezeichneter Ansatz zur komponentenorientierten Modularisierung von Fehlerbäumen vorgeschlagen. Darauf aufbauend wird in [Kaiser06] die Methode der State-Event-Fault-Trees (SEFT) vorgestellt, mit der kausale Abläufe in modularisierten Fehlerbäumen behandelt werden können.

2.3.2 Qualitative Methoden

Eine verbreitete qualitative Methode zur Fehlermodellierung ist die Fehlermöglichkeits- und Einflussanalyse (FMEA), unter anderem nach [MIL-STD-1629A:49, VDA-Band4-FMEA:06, DGQ-Band13-11:12]. Dieselbe Methode wird in [DIN-EN-60812:06] als Fehlzustandsart- und Auswirkungsanalyse dargestellt. Für diese erfolgt eine systematische Zusammenstellung eventueller Fehlzustände der einzelnen Komponenten, aus welchen anschließend mögliche Folgen für das System abgeleitet werden. Dabei werden Tabellen erstellt, die mögliche Fehlzustände, sowie deren Ursachen, Folgen und Konsequenzen in Bezug auf den Systembetrieb auflisten. Anhand dessen wird die Kritikalität aus Bewertungen der Ursachenwahrscheinlichkeit und Auswirkungsschwere bemessen. Außerdem wird ein Faktor für die Möglichkeit der Entdeckung vor Eintreten des Fehlers eingeschätzt. Bei kritischen Punkten werden notwendige Verbesserungsmaßnahmen definiert.

Im Wesentlichen liegt der Unterschied zwischen den Verfahren zur Fehlermodellierung der FMEA und FTA darin, dass in ersterer von Ursachen ausgehend Folgen festgestellt werden (Bottom-Up-Prinzip). Bei der FTA hingegen werden von Folgen ausgehend mögliche Ursachen hierfür ermittelt (Top-Down-Prinzip). Außerdem können in der FMEA mehrere Folgen für je eine Ursache angegeben werden, anstatt jeweils einer einzelnen in der FTA. Zudem ist die klassische und gebräuchliche Definition der FMEA qualitativ, während die der FTA hingegen auch probabilistische Auswertungen erlaubt. Zwar werden in der FMEA auch Wahrscheinlichkeitswerte für Fehlerursachen abgeschätzt. Die Beziehungen der Fehlermodelle werden jedoch nicht zu einer arithmetischen Auswertung genutzt, weswegen keine Wahrscheinlichkeiten für Fehlerfolgen aus den Modellen ermittelt werden.

Eine gebräuchliche Variante der FMEA nutzt sogenannte Fehlernetze [VDA-Band4-FMEA:06, DGQ-Band13-11:12], was nachfolgend vereinfachend als auf Fehlernetzen basierte FMEA (FN-FMEA) bezeichnet wird. Die FN-FMEA stellt auf eine graphisch formalisierte Zuordnung von Fehler- und Folgezuständen ab, die durch die Fehlernetze (s. Bild 2.5) visualisiert werden.

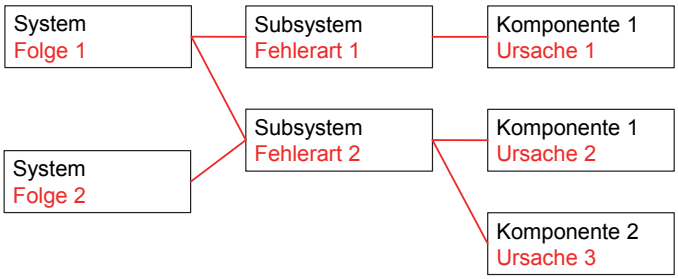


Bild 2.5: Prinzipschema des Fehlernetzes der FN-FMEA

Der Formalismus der Fehlernetze ist jedoch nicht wie der FTA im Sinne einer Algebra untermauert, weswegen kein herkömmliches Verfahren zu deren probabilistischer Auswertung existiert. Auch in informativer Hinsicht werden die in Fehlernetzen modellierten systematischen Gruppierungen von Fehlern gleicher Auswirkung nicht entsprechend genutzt, um Schlussfolgerungen aus der Menge aller Ursachen zu extrahieren. Dies bedeutet, dass sowohl Wahrscheinlichkeiten, als auch die Anzahl möglicher Ursachen nicht zur Beurteilung einer Fehlerfolge auf Systemebene verwendet werden. Somit sind die FMEA und die FN-FMEA sowohl in Hinsicht auf die numerische, als auch auf die aussagenlogische Auswertung qualitativer Art.

2.3.3 Quantitative Ansätze der FMEA

Eine Reihe veröffentlichter Ansätze setzt an dem Punkt an, das FMEA-Tabellenschema zu einer probabilistischen Auswertung zu nutzen. Ein solcher Ansatz ist die FMECA (Failure Modes Effects and Criticality Analysis) [MIL-STD-1629A:80], die erstmals im Jahr 1949 veröffentlicht wurde. Für diese ist auch die Bewertung der Wahrscheinlichkeiten von Fehlerfolgen definiert, indem die Wahrscheinlichkeit einzelner Fehlerursachen und die bedingte Wahrscheinlichkeit der Folge eines kritischen Fehlers berechnet werden. Alle zur gleichen Folge beziehungsweise gleichermaßen schwerwiegenden Folgekategorie führenden Wahrscheinlichkeiten werden dem Ansatz nach miteinander addiert.

In [Price98] wird die Betrachtung von Fehlerkombinationen innerhalb der FMEA ebenfalls thematisiert, sowie ein Schema zu deren Überführung in Fehlerbäume. Darin wird jedoch nur von der ursprünglichen, rein tabellarischen Form der FMEA ausgegangen, sodass keine ko-

härenten formalen Modelle zur Repräsentation logischer Beziehungen und deren probabilistischer Interpretation dort behandelt werden.

In [Pickard05, Xiao11] wurden aufeinander aufbauende Ansätze zur sogenannten Multiple FMEA vorgestellt. Darin werden die Beziehungen der FN-FMEA als logische Zuordnungen von Fehlerursachen zu Fehlerfolgen interpretiert, sodass diese im Stil der FTA-Modelle dargestellt werden. Fehlerkombinationen können in dem Zuge zusätzlich zu den Einzel-Fehlerbeziehungen der FMEA angegeben werden. Für jeden Zustand des Gesamtsystems wird dazu ein separater Fehlerbaum erzeugt. Die Auswertung der Fehlermodelle erfolgt indes hinsichtlich des qualitativen Parameters der Kritikalität.

Die probabilistische FMEA (pFMEA) [Grunske07] berücksichtigt die Übergangswahrscheinlichkeiten der Zustandsübergänge zwischen Funktionsfähigkeit und Fehlzuständen. Dabei liegt hier kein graphischer Formalismus für ein Fehlermodell zugrunde. Die Wahrscheinlichkeiten der Folgezustände des Systems werden aus den Übergangswahrscheinlichkeiten zwischen möglichen Zuständen der Einzelbestandteile des Systems mittels stochastischer Simulationsverfahren approximiert.

In [Kaiser15] wird die als probFMEA bezeichnete probabilistische Erweiterung der Fehlernetze der FN-FMEA dargestellt. So können durch ergänzende Formalismen innerhalb eines Fehlernetzes logische Beziehungen im Sinne der UND-, ODER- und NICHT-Operatoren ausgedrückt werden. Zudem wird vorgeschlagen, Ursache-Folge-Kausalitäten mit bedingten Wahrscheinlichkeiten anzugeben, sodass die Wahrscheinlichkeit von Folgen entsprechen differenziert behandelt werden kann. Die Auswertung der Beziehungsstrukturen erfolgt mittels mehrwertiger Entscheidungsdiagramme [Zocher05].

2.3.4 Methodische Ansätze zur Mehrzustands-Fehlermodellierung

Die Mehrzustands-Zuverlässigkeit wurde beginnend mit [Barlow78, El-Neweihi78a, El-Neweihi78b] als Frage der Zuverlässigkeitstheorie bearbeitet [Aven99, Misra08, Lisnianski10, Levitin11]. In [Yingkui12] findet sich eine Übersicht über den Stand und die Errungenschaften dieser Bestrebungen bis dato. Ziel dieses Arbeitsfelds ist die Betrachtung der Zuverlässigkeit von Systemen mit Unterscheidung zwischen mehreren Fehlzuständen, im Gegensatz zu dem binären Ansatz mit den Zuständen der Funktion beziehungsweise des Ausfalls. So werden Komponenten mit mehreren Fehlzuständen und daraus resultierend mehreren möglichen Fehlzuständen in Zuverlässigkeitsmodellen probabilistisch dargestellt und berechnet.

Die Mehrwertigkeit dieser methodischen Ansätze bezieht sich dabei allerdings auf technisch-funktionale Zustände des Systems und dessen Bestandteile. Die logische Grundlage hingegen beruht auf Zweiwertigkeit, da für das Zutreffen oder Nicht-Zutreffen von Aussagen über Zustände und Folgen stets die Kriterien {‚$wahr$'} und {‚$falsch$'} angewendet werden. Es besteht demnach kein Konflikt hinsichtlich der Einwände bezüglich verfügbarer Ansätze für mehrwertige Logik nach [Jaynes03] (s. Kapitel 2.1).

Auch für die Methoden der FTA und RBD existieren Ansätze zur Behandlung der Mehrzustands-Zuverlässigkeit, beispielsweise in [Caldarola80, Wood83, Xizhi84, Wood85, Lisnianski07]. So werden in Mehrzustands-RBD mehrere Fehlzustände und Folgen betrachtet. Vergleichbar hierzu werden für die Mehrzustands-FTA mehrere Hauptereignisse (Top-Level-Events) definiert. Dabei werden jedoch keine integralen Modelle erstellt, die alle Zustandskombinationen miteinander verbinden. Eine Ausnahme darunter stellt der Ansatz von [Lisnianski07] dar, der ein in RBD integriertes Mehrzustandsmodell vorschlägt, das mittels stochastischen Simulationsverfahren ausgewertet wird.

Eine mengentheoretische Veranschaulichung der Mehrzustands-Zuverlässigkeit wurde in [Xizhi84] im Rahmen der Erarbeitung eines Konzepts zur Mehrzustands-Fehlerbaumanalyse verwendet. In dieser werden ebenfalls Hauptereignisse definiert. Für diese Ereignisse auf Systemebene werden Mengendiagramme für zwei allgemeine Fälle dargestellt und diskutiert, nämlich sich gegenseitig ausschließender beziehungsweise sich überschneidender Folgeereignisse.

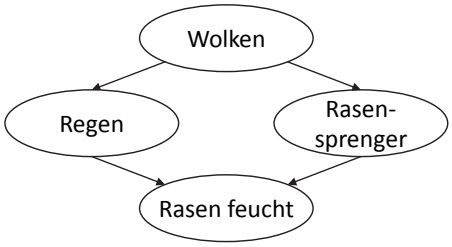
2.3.5 Ereignisbaumanalyse

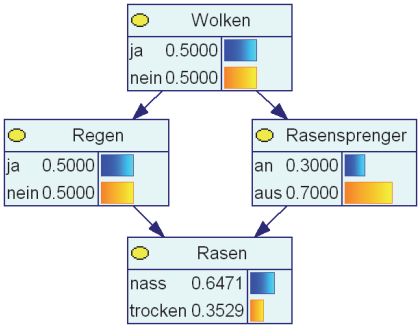
Mit der Ereignisbaumanalyse (ETA, englisch: Event Tree Analysis) oder Ereignisablaufanalyse [DIN62502:11] existiert außerdem eine probabilistische Methode zur Modellierung unerwünschter Ereignisse und solcher Begebenheiten, die im Kontext des Betriebs des Systems zu diesen führen können. Dies ist keine Methode zur Erarbeitung von Fehlermodellen im engeren Sinn, die ein System umfassend repräsentieren. Stattdessen ist der Betrachtungshorizont erweitert, sodass selektierte Ereignisszenarien und Konstellationen diverser möglicher Begebenheiten untersucht werden, unter anderem Koinzidenzen spezieller Betriebsereignisse mit Komponentenfehlern im System betrachtet. Für die Methodik der ETA ist eine differenzierte probabilistische Bewertung möglicher alternativer Ausgänge auf Basis bedingter Wahrscheinlichkeiten definiert. So können dabei Werte der Wahrscheinlichkeit für das Eintreten verschiedener Folgen angegeben werden sowie eines Ereignisablaufs ohne kritische Konsequenzen.

2.4 Methoden auf Basis Bayesscher Netzwerke

Pearl schlug in dem Artikel „Reverend Bayes on Inference Engines: A Distributed Hierarchical Approach“ [Pearl82] ein Schema probabilistischer Inferenznetzwerke aus Beziehungen zwischen mehreren Zufallsgrößen erstmals vor. Mit Bezug auf die darin umgesetzte Wahrscheinlichkeitsauffassung nach [Bayes1763] wurde dies später als Bayessches Netzwerk (BN) bezeichnet [Pearl85]. Das Schema wurde unter anderem in [Kim83, Pearl88, Pearl00] weiter ausdefiniert. Eine anschauliche Erläuterung findet sich unter anderem in [Charniak91, Darwiche08]. Umfassende Arbeiten hierzu sind beispielsweise [Whittaker90] zur Anwendung graphentheoretischer Modelle in multivariater Statistik sowie [Russell95] zu probabilistischem Schlussfolgern mit BN.

BN bestehen aus gerichteten azyklischen Graphen, deren Knoten diskrete Zufallsvariablen darstellen. Für jeden solchen Knoten gilt, dass die durch ihn repräsentierte Zufallsgröße auf der Basis von mindestens zwei diskreten Zuständen aufgebaut ist. Mittels gerichteter Kanten (Pfeile) zwischen den Knoten bilden diese ein Netzwerk, das bedingte Abhängigkeiten der jeweiligen Zielknoten (Kindknoten) von den Ausgangsknoten der Pfeile (Elternknoten) symbolisiert (s. Bild 2.6, oben). Sie stellen dadurch probabilistische Einflüsse einzelner Größen auf andere dar.





Regen	Wolken	keine Wolken
ja	0,8	0,2
nein	0,2	0,8

Rasen-sprenger	Wolken	keine Wolken
an	0,1	0,5
aus	0,9	0,5

Rasen	Sprenger an		Sprenger aus	
	Regen	kein Regen	Regen	kein Regen
nass	0,99	0,9	0,9	0,0
trocken	0,01	0,1	0,1	1,0

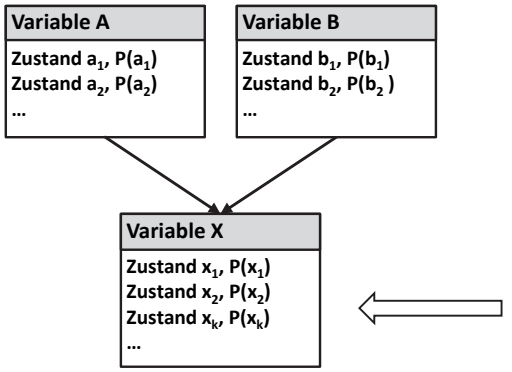
Bild 2.6: allgemeines Beispiel für BN nach [Russell95, Murphy98] (oben); Berechnung in [GeNIe10] (unten, links) und Tabellen bedingter Wahrscheinlichkeiten CPT (unten, rechts)

Die individuellen Abhängigkeiten der Zustände eines Kindknotens von dessen Elternknoten werden im Einzelnen jeweils in einer Tabelle bedingter Wahrscheinlichkeiten (CPT, englisch: Conditional Probability Table) für jeden Knoten angegeben (s. Bild 2.6 unten rechts). In den

CPT werden alle Zustandskombinationen der darauf gerichteten Elternknoten gebildet und den Zuständen des Zielknotens (Kindknoten) zugeordnet. Diese Zuordnung geschieht durch jeweils eine bedingte Wahrscheinlichkeit die ausdrückt, wie wahrscheinlich ein Zustand des Kindknotens ist, gesetzt den Fall, dass eine bestimmte Kombination von Zuständen der Elternknoten vorliegt.

Nach Pearl handelt es sich bei den Kanten der BN um Beziehungen zwischen den Elternknoten $A, B, \ldots$ und Kindknoten X um logische Zusammenhänge in Form von „wenn a_i…-dann x_i…"- [Pearl82]. Durch die bedingten Wahrscheinlichkeiten in CPT wird laut Pearl Ungewissheit (übersetzt aus dem Englischen: „Uncertainty") in diesen Regeln abgebildet.

Links in Bild 2.7 sind beispielsweise die Wahrscheinlichkeiten der Zustände eines Kindknotens X von den Wahrscheinlichkeiten der Zustände der Elternknoten A und B abhängig dargestellt. a_i und b_j sind in den Elternknoten enthaltene Einzelwerte. Jedes x_{ij} in der CPT rechts in Bild 2.7 ist eine bedingte Wahrscheinlichkeit $P(x_{ij}|a_i \cap b_j)$, die den Wahrscheinlichkeitswert darstellt, mit dem der einzelne Zustand x_{ij} logisch zutreffend ist, wenn a_i und b_j zutreffen.



A➔	a_1		a_2	
B➔	b_1	b_2	b_1	b_2
AxB➔	$a_1 \cap b_1$	$a_1 \cap b_2$	$a_2 \cap b_1$	$a_2 \cap b_2$
<Variable X>	Bedingungen			
<Zustand x_1>	$P(x_1 \mid a_1 \cap b_1)$	$P(x_1 \mid a_1 \cap b_2)$		
<Zustand x_2>	$P(x_2 \mid a_1 \cap b_1)$	...		...
<Zustand x_k>			$P(x_k \mid a_i \cap b_j)$	
...	...			...

Bild 2.7: Inhalte der BN-Netzwerkelemente: Aufbau der in Knoten repräsentierten Zufallsgrößen (links im Bild) und Tabelle bedingter Wahrscheinlichkeiten (CPT) (rechts im Bild)

Die Wahrscheinlichkeitsverteilung eines Kindknotens ergibt sich abhängig von der Gesamtheit aller bedingten Wahrscheinlichkeiten in der CPT, sowie dem Schnitt (Konjunktion) der Elternknoten und der Überlagerung deren Wahrscheinlichkeitsverteilungen (englisch: „Joint Probability Distribution" [Pearl00]) auf Basis der Gleichung:

$$P(A, B, \ldots, X, Y) = \prod_i P(Y \mid A, B, \ldots X) \tag{2.21}$$

So kann ein BN üblicherweise anhand des Multiplikationssatzes algebraisch aufgelöst werden [Pearl00], wie beispielsweise für obiges Netzwerk mit den Knoten A, B und X:

$$P(A,B,X) = P(A)\,P(B|A)\,P(X|A,B) \tag{2.22}$$

In [Lauritzen88] wurde das laut [Weber06] klassische exakte Lösungsverfahren des Clustering-Algorithmus für BN vorgestellt. In diesem graphentheoretisch begründeten Verfahren werden die Knoten eines BN auf spezielle Weise gruppiert, sodass anschließend eine exakte Berechnung erfolgen kann. Statistische Abhängigkeiten werden dabei kompensiert, ohne dass einzelne Terme hinsichtlich minimaler Schnittmengen (englisch: Minimal-Cut-Sets) auszuwerten sind, wie dies für die algebraische Auswertung von logischen Termen typischerweise der Fall ist. Es gibt zudem weitere exakte und ferner auch approximative Verfahren, die mitunter erweiterte Funktionalitäten ermöglichen [Darwiche08, Mateescu10]. Für diese Arbeit genügt die Verwendung eines einzelnen exakten und bewährten Berechnungsverfahrens. So wird nachfolgend der Clustering-Algorithmus zur Berechnung von BN verwendet, der unter anderen im BN-Anwendungsprogramm [GeNIe10] implementiert ist.

Im Kontext der Lösungsalgorithmik für BN wurde in [Darwiche02] ein Ansatz vorgestellt, der sich auf die spezifischen logischen Zusammenhänge zwischen Zuständen von Eltern- und Kindknoten stützt. Dabei wird gezeigt, dass die Inferenz in BN auf den Grundverfahren der logischen Algebra, der Konjunktion und Diskunktion, beruht. Das Verfahren jedoch beschränkt sich auf zweiwertige Zufallsvariablen mit nur binären Werten bedingender Einflusswahrscheinlichkeiten. In [Poon11] wurde das als „Sum-Product Network" bezeichnete Schema zur graphischen Darstellung vorgeschlagen, dass sich auf die Arbeit in [Darwiche02] bezieht und diesen entspricht. Soweit es den Grundgedanken der Veranschaulichung betrifft ist dies analog zu der in Kapitel 5.3.3 verwendeten Veranschaulichung der in dieser Arbeit behandelten Fragestellungen. Nähere Einzelheiten sind dort erläutert.

Die Anwendung von BN im Gebiet der technischen Zuverlässigkeit wurde in [Barlow88, Almond92] erstmalig vorgeschlagen. Die seither veröffentlichten Beiträge zu der Thematik umfassen ein breites Spektrum an Ansätzen und Fragestellungen, was in [Langseth07, Langseth08, Weber10, Weber12] vergleichsweise übersichtlich nachvollziehbar ist. Von speziellem Interesse für diese Arbeit sind darunter solche Ansätze, die Fehlermodelle in der Art von klassischen Methoden zur Fehlermodellierung in BN umzusetzen.

So zeigt [Torres98] die Ermittlung der System-Fehlerwahrscheinlichkeit auf Basis von BN nach dem methodischen Prinzip der RBD. Weitere Beiträge zur Zuverlässigkeitsmodellierung mit BN und Bezug zu RBD sind ferner [Zhou06, Simon07, Mi12]. In [Castillo97] wurden erstmalig Analogien zwischen BN Zuverlässigkeitsmodellen und Fehlerbäumen behandelt. In [Portinale99] werden die Implementierung logischer Operationen als BN-Knoten und die

Transformation von Fehlerbäumen in BN gezeigt, was nachfolgend in [Bobbio01, Portinale05, Lampis09, Khakzad11] aufgegriffen und weitergeführt wurde. [Weber03, Boudali04, Boudali05, Montani05, Boudali06] zeigen, dass auch die Fehlermodelle der advanced FTA in einem dynamischen Ansatz der BN (dBN) [Dean89, Murphy02] in vorteilhafter Weise umsetzbar sind [Portinale10, Marquez10]. Ein prinzipiell vergleichbarer Ansatz zur Modellierung der Zuverlässigkeit auf Basis zeitabhängiger BN-Fehlermodelle ist in [Arroyo92] beschrieben, der methodisch nicht spezifisch formalisiert ist. Für diesen wurde vorrangig die Nutzung des probabilistischen Modells zur Vorhersage und Diagnose behandelt.

[Lee99a, Lee99b, Lee01, Lee02] zeigte den ersten Ansatz zur probabilistischen Modellierung der Fehlerursache- und Fehlerauswirkungsbeziehungen als BN im Zuge der FMEA-Methodik. Dabei werden teilweise Mehrzustandsgrößen für Komponenten und Ereignisse verwendet. Der Aufbau des Netzwerks zielt vorrangig auf die Modellierung unerwünschter Ereignisse ab, die jeweils als ein Netzwerkknoten dargestellt werden. So wird ein Analysemodell in [Lee02] als Nutzungsszenario bezeichnet (übersetzt aus dem Englischen: „use case“) (s. Bild 2.8).

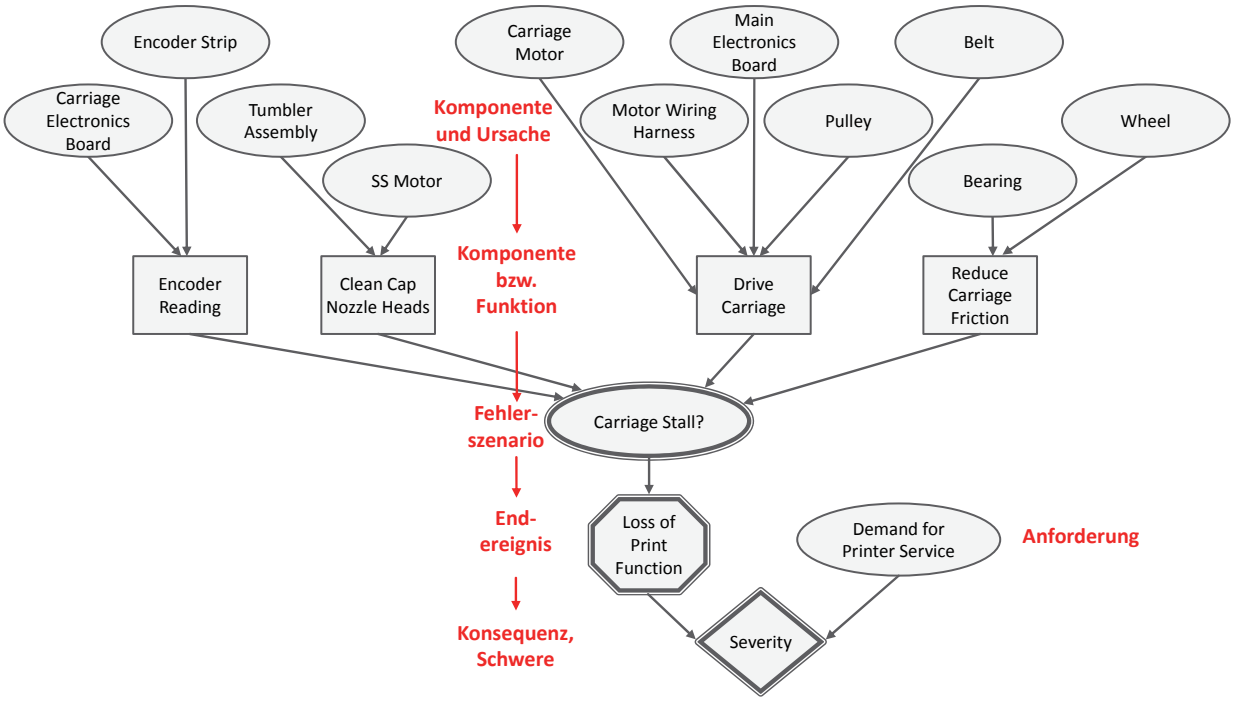


Bild 2.8: Beispiel eines Netzwerk-Modells der BN-FMEA auf Basis von [Lee02]

Verschiedene Aspekte der Thematik werden in hierzu vergleichbaren Ansätzen durch [Kempf01, Kempf08, Chen10, García11] dargestellt. Diese verwenden binäre Zustände der Variablen in den Netzwerkknoten, sodass ein Knoten für einen Fehlermodus oder eine Fehler-

wirkung steht, für den die Wahrscheinlichkeit des Zutreffens und Nicht-Zutreffens bestimmt wird.

In [Boissou03] wird ein Ansatz zur Betrachtung der Mehrzustands-Zuverlässigkeit eines Systems in BN beschrieben. Darin wird das System als ein Mehrzustands-Netzwerkknoten ausgeführt. Die untergeordneten Knoten hingegen repräsentieren Bauteile auf der untersten Hierarchieebene des Netzwerks. In den Zwischenebenen werden funktionale Zusammenhänge durch logische Gatterknoten dargestellt, die die jeweils binären Komponentenzustände zu Aussagen über den Systemzustand verarbeiten. [Zhou06] verwendet einen ähnlichen Ansatz, wobei darin auch Unterkomponenten mit jeweils mehreren Zustandsmöglichkeiten umgesetzt sind. Aufgrund der Restriktionen der RBD-Methodik und der Ansätze der Mehrzustands-Zuverlässigkeit bildet das Modell stets ein spezifisches Merkmal der Systemeigenschaften, beispielsweise die Funktions- oder Leistungsfähigkeit ab. Zudem erfolgt die hierarchische Gliederung des BN-Fehlermodells in [Zhou06] anhand der Darstellung im zugehörigen RBD, die sich nach logisch-funktionalen Bedingungen richtet. In dem darauf bezogenen Verfahren in [Mi12] werden in einem ähnlichen Modellansatz wiederum spezifische logische Operationen ähnlich zur FTA als dedizierte BN-Knoten dargestellt. [Zhai13] schlägt BN-Fehlermodelle in einem Mehrzustands-FT vor, die auf einzelne binär bewertete Fehlersymptome als Basisgrößen aufbauen. [Cao16] zeigt ferner ein Mehrzustands-Zuverlässigkeitsmodell, das sich teilweise an Komponenten des Systems orientiert, die im Sinne der Mehrzustands-Zuverlässigkeit aufgebaut sind. Andere Knoten im Netzwerk sind dagegen funktional orientiert, sodass kein integrales Modell aufgrund der Systemstruktur dabei entsteht. Stattdessen mimt das Modell einen Mehrzustands-Fehlerbaum. Daher unterliegt auch dieser Ansatz der Beschränkung der Darstellbarkeit der Kombination weniger Fehlzustände im Rahmen einer ausgewählten Systemeigenschaft.

Die in diesem voranstehenden Teilabschnitt gegebenen Ausführungen stellen einen gestrafften Überblick über die verschiedenen Strömungen und Arbeiten in dem Teilgebiet der Fehlermodellierung mit BN dar. Nähere Details zu deren Eigenschaften werden im Kontext der jeweils zutreffenden Folgeabschnitte an gegebener Stelle vertieft diskutiert.

3 Wissenschaftlicher Ansatz

In dieser Arbeit wird die probabilistische Grundlage zur Darstellung integraler Mehrzustands-Fehlermodelle komplexer technischer Systeme behandelt, die die Möglichkeiten zur Modellierung und Auswertung gegenüber den bisherigen methodischen Ansätzen dieser Art grundlegend erweitert. Der in [Rauschenbach15] gezeigte Ansatz auf Basis Bayesscher Netzwerke (BN) dient dazu als Anhaltspunkt für dessen grundlegende wahrscheinlichkeitstheoretische Erschließung und Verifikation. Dazu werden benötigte probabilistische Zusammenhänge, die bislang nicht verfügbar sind, zunächst theoretisch erschlossen. Begleitend wird ein eingangs entwickeltes methodisches Rahmenkonzept für einen dementsprechenden Ansatz zur Fehlermodellierung aufgebaut. In diesem werden die in den theoretischen Herleitungen erreichten Erkenntnisse anschließend auf die Fehlermodellierung technischer Systeme angewandt und abschließend in einem konkreten Anwendungskontext charakterisiert und diskutiert.

Aus übergeordneter Sicht betrachtet unterscheidet sich der Ansatz dieser Arbeit von denjenigen der Mehrzustands-Zuverlässigkeit dadurch, dass dieser einfachere und intuitiv nachvollziehbare Gleichungssysteme verwendet. Dies gelingt durch einen zu den gebräuchlichen Termen für logische Operationen unterschiedliche Formulierung in der disjunktiven Normalform. Dies wird mengentheoretisch für Modelle aus Mehrzustands-Zufallsgrößen dargelegt. Die Auswertung dieser Modelle kann zudem im Zuge einer methodisch anschaulichen Umsetzung in BN-Modellen erfolgen. Ferner ist die bisher übliche Beschränkung auf eine oder wenige einzelne funktionsbezogene Fragestellungen des Modells nicht prinzipiell erforderlich.

3.1 Abgrenzung der Arbeit gegenüber dem Stand der Wissenschaft und Technik

Die Herangehensweise und der methodische Ansatz dieser Arbeit lassen sich gegenüber den bisher gebräuchlichen anhand mehrerer Aspekte abgrenzen:

Konkrete logische Beziehungen auf Grundlage einzelner Werte der mehrwertigen Zufallsgrößen in BN werden im Hinblick auf die Fehlermodellierung nachgewiesen, was bislang generell und insbesondere im Kontext der technischen Zuverlässigkeit nur in begrenztem Maß betrachtet wurde. Diese aussagenlogischen Beziehungen werden in dieser Arbeit auf Basis einer spezifisch angepassten mengentheoretischen Betrachtungsweise aussagenlogisch und algebraisch nachvollzogen. Für diesen Ansatz werden die Grundlagen von Mengendiagrammen nach [Euler1761, Venn1880] auf die integrale Betrachtung

mehrwertiger Zufallsgrößen in einer weitergehenden Weise bezogen, als dies in [Pfeiffer65, Vesely81] bislang gezeigt wurde. Die stochastischen Abhängigkeiten zwischen Einzelwerten der Zufallsgrößen werden dabei in Bezug auf Logikkalkül und Wahrscheinlichkeitsarithmetik charakterisiert. Nachfolgend wird aufgezeigt, dass und wie die Axiome Boolescher Logik [Peano1888] unmittelbar auf das Gleichungssystem eines BN anwendbar sind.

Den eingangs vorgestellten Arbeiten zur Umsetzung von FMEA und FTA als BN liegt kein Ansatz zugrunde, der ein System zusammenhängend abbildet. In den RBD-artigen Ansätzen ist eine integrale Repräsentation des Systems bedingt durch die Definition der Basismethode zwar gegeben, wird aber als Einziges in [Zhou06] in entsprechend integraler Weise aufgegriffen. Allerdings kann vergleichbar zu den generischen Ansätzen der Mehrzustands-RBD nur eine Systemeigenschaft in abgestufter Weise dargestellt werden, da nach dem RBD-Ansatz im regulären Fall je ein spezifisches Blockmodell als Ausdruck für jeweils eine spezifische Fragestellung benötigt wird. Der systemisch-integrale Ansatz der Arbeit stellt einen umfassenderen Lösungsansatz hierfür dar.

Im Vergleich zu [Xizhi84, Darwiche02, Pearl00, Poon11] erlaubt der Ansatz dieser Arbeit eine umfassendere Differenzierung logischer und funktionaler Zusammenhänge in mehrwertigen Zustandsnetzwerken beziehungsweise Fehlermodellen, die auf graphisch formalisierten logischen Strukturen beruhen. Ein Beispiel hierfür sind Mehrzustands-Fehlerbäume nach [Xizhi84]. Abhängigkeiten innerhalb der Vernetzung von Fehlerursachen und –folgen werden konkret anhand der Beziehungen zwischen den Einzelwerten der Mehrzustands-komponenten betrachtet. Zudem erfolgt deren anschauliche Interpretation hinsichtlich des kausalen Rahmens technischer Fehler in Systemen. Es wird eine methodische Umsetzung von Mehrzustands-Fehlermodellen zusammenhängender Gesamtsysteme mittels BN-Modellen algebraisch untersucht und probabilistisch plausibilisiert. Die Modelltopologie des methodischen Ansatzes ist dabei dem Stil der FN-FMEA entlehnt und folglich mehrstufig strukturhierarchisch gegliedert. Jede Zufallsgröße repräsentiert dabei eine abgrenzbare Komponente. Einzig in [Bobbio01, Portinale15] wird solch eine systemhierarchische Modellstruktur zugrunde gelegt und zudem eine Mehrzustandsmodellierung vorgeschlagen. Letztere wird jedoch nicht im Detail konkret vorgestellt und untersucht, was im Zuge dieser Arbeit jedoch erfolgt.

Zur Darstellung multipler Fehlerbeziehungen als Folgen beliebiger Zustandskonstellationen existieren jedoch kein gesamtheitliches Modellkonzept und kein darauf bezogenes integrales aussagenlogisches Modell. Wie im Zuge der Arbeit gezeigt wird, lässt sich dies in BN

darstellen. Ferner wird gezeigt, wie alternative Folgemöglichkeiten mittels bedingter Wahrscheinlichkeiten im Modell repräsentiert werden können. Dies wurde zwar vereinzelt bereits in verschiedenen Methoden erwähnt [MIL-1629A:80, DIN-25419:85, Bobbio01, Lee02, Kaiser06, Weber06, Khakzad11, Kaiser15]. Jedoch werden dort der algebraische Hintergrund und die konsistente Nutzung in Gesamt-Fehlermodellen nicht aufgezeigt.

Anhand der erarbeiteten algebraischen Grundlage erfolgt zudem eine Validierung der Verwendung exakter BN-Lösungsalgorithmen im Anwendungskontext der System-Fehlermodelle. Dabei werden stochastische Abhängigkeiten in zuverlässigkeitstechnischer Hinsicht insbesondere anhand der Fehlerkategorien nach [Vesely81] charakterisiert. Dies ist in FMEA-inspirierten Methoden auf Basis von BN bislang nicht erfolgt.

3.2 Wissenschaftliche Methodik

Angesichts dieser Ausgangssituation besteht der wissenschaftlich-methodische Ansatz für die Arbeit darin, die korrekte Darstellung, Interpretation und Auswertung aussagenlogischer Zuordnungen zwischen Fehlerursachen und Folgezuständen als Bestandteil eines integralen Fehlermodells eines Systems aufzuzeigen. Die methodischen Mittel dabei sind in der Hauptsache algebraischer und mathematischer Art, was die Herleitung der arithmetischen Grundlage und der probabilistischen Auswertung der Netzwerke betrifft. Bezüglich des Rahmenkonzepts und der Beantwortung der Fragestellungen hinsichtlich deren geeigneter und zielführender Anwendung beruht die Methodik auf technologisch-systemtheoretischer Anschauung. Die Priorität wurde auf die intuitive Darstellung und Interpretation der aussagenlogischen und kausalen Zusammenhänge gelegt. Dies erhöht die unmittelbare Nachvollziehbarkeit der Grundlagen und begünstigt dadurch deren Umsetzung im methodischen Konzept. Zudem unterstützt dies die nachfolgende Übertragung auf den Anwendungskontext.

Der Schwerpunkt der Arbeit liegt im probabilistisch-methodischen Konzept, um charakteristische Ursache-Folge-Schemata von Fehlzuständen technischer Produkte modellhaft behandeln zu können. Daher ist der Ausgangspunkt der Arbeit das Postulat, dass der Ansatz der logisch-probabilistischen Modellierung entsprechender Eigenschaften und Wirkungen in Systemen prinzipiell zulässig und korrekt ist. Zudem werden allgemeine Grundlagen der Zuverlässigkeitstheorie als gültig in Anspruch genommen. Somit wird davon ausgegangen, dass der gebräuchliche logisch-probabilistische Basisansatz valide ist und sich das reale Systemverhalten in entsprechenden Modellen hinreichend korrekt schematisiert ausdrücken lässt. Dies wird im Zuge der Arbeit nicht grundlegend in Frage gestellt.

3.3 Relevanz fundamentaler Problemstellungen der Probabilistik

In der Wahrscheinlichkeitstheorie und Statistik sind Kausalität und Induktion fundamentale Aspekte hinsichtlich der Möglichkeit von Schlussfolgerungen und Ableitung von Aussagen. Sie bestimmen über die Zulässigkeit von Verfahren und Gültigkeit der Ergebnisse. Mit Blick auf die in dieser Arbeit behandelte Themenstellung der Fehlermodellierung schließen sich diese als Faktoren für die Problemstellung dieser Arbeit aus, wie in den folgenden Unterabschnitten begründet wird.

3.3.1 Kausalität in Fehlermodellen

Im Zuge der allgemeinen Verwendung von BN zur Analyse statistischer Daten ist Kausalität [Pearl00] ein zentraler Ausgangspunkt für wissenschaftliche Auseinandersetzungen [Hitchkock10]. Bei der Gewinnung von Modellen aus statistischen Daten, deren Interpretation und der Ableitung von Schlussfolgerungen ist zu unterscheiden, worin der Grund für beobachtete Korrelationen zwischen verschiedenen Größen liegt. So sind in Daten feststellbare Zusammenhänge zwischen Wahrscheinlichkeitswerten nicht zwingend kausal bedingt.

Beispielsweise können in einer statistischen Studie Zeiträume erkannt werden, in welchen zugleich ein signifikant erhöhter Konsum von Speiseeis beobachtet wird und zugleich eine signifikant erhöhte Zahl von durch Sonnenbrand geschädigten Menschen registriert wurde. Tatsächlich ist es nicht das Nahrungsmittel, das den Sonnenbrand verursacht und auch umgekehrt scheint die Folgerung unplausibel, ein Sonnenbrand bewirke das Bedürfnis nach Speiseeis. Vielmehr sind Zeiträume entsprechender Wetterbedingungen der Hintergrund der Koinzidenzen erhöhter Fallzahlen von Sonnenbränden und gesteigerten Speiseeiskonsums.

Diese Problematik lässt sich mit der Begründung von dem thematischen Rahmen dieser Arbeit abgrenzen, dass keine Annahmen über mögliche technische Zusammenhänge aus statistischen Daten induktiv abgeleitet werden. Stattdessen werden die Einflussbeziehungen ausschließlich aus technisch-kausalen Gesetzmäßigkeiten in deduktiver Weise ermittelt. Die Kausalität der Fehlermodelle wird dabei nicht aus Korrelationen zwischen statistischen Daten herausgearbeitet, sondern aus technologischen Kenntnissen über Fehler, Wirkeffekte und Folgen. Daher wird das logische Modell unmittelbar und ausschließlich aus kausalen Zusammenhängen gebildet, weswegen es uneingeschränkt zur probabilistischen Auswertung genutzt wird.

3.3.2 Deduktive und induktive Suchstrategien zur Fehlermodellierung

In philosophischer Hinsicht bezeichnen Deduktion und Induktion die Vorgehensweise der Schlussfolgerung aus gegebenen Informationen. Bei der Deduktion werden aus gegebenen Eingangsinformationen nach bekannten Gesetzen zulässige Schlussfolgerungen abgeleitet. Bei der Induktion wird hingegen aus gegebenen Sätzen von Eingangsinformationen und jeweils zutreffenden Schlussfolgerungen auf die dahinterliegende Regel zurückgeschlossen.

Es ist üblich, die Verfahren der Fehlermodellierung in deduktive und induktive Methoden einzuteilen, wie beispielsweise in [Vesely81, Bertsche04, Stapelberg09, Werdich12]. Dieser Wortgebrauch bezüglich der Methoden entspricht nicht deren Bedeutung im Kontext der Aussagenlogik. Zu deduktiven Methoden wird beispielsweise die FTA gezählt, da ausgehend von Folgen nach möglichen Ursachen gesucht wird. Demgegenüber gilt beispielsweise die FMEA als induktive Methode, da ausgehend von Fehlerursachen nach deren Folgen gesucht wird. In Bezug auf die Fehlermodellierung bezeichnen die Begriffe die Systematik der Vorgehensweise zur Systemanalyse. Dabei werden aber stets geltende Gesetzmäßigkeiten zugrunde gelegt, was in beiden Fällen einer Deduktion im philosophischen Sinn entspricht. Es werden hingegen im Kontext dieser Methoden keine Gesetzmäßigkeiten aus empirischen Daten induktiv gefolgert, um die Modellstruktur hieraus abzuleiten. Die Analysestrategien sowohl deduktiver, als auch induktiver Methoden zur Fehlermodellierung beruhen demnach auf logischer Deduktion. Dies entspricht der Aussage Jaynes, dass dies im Rahmen der Laplaceschen Wahrscheinlichkeitstheorie grundsätzlich der Fall ist [Bretthorst14] (vgl. Kap.2.1).

Aus einem anderen Betrachtungswinkel bedeutet dies, dass die methodische Fehlermodellierung nicht der Beantwortung der Frage dient, ob es einen Zusammenhang zwischen beobachteten Fehlerphänomenen gibt. Stattdessen ist es deren Zweck, zu bewerten, wie wahrscheinlich ein bereits zuvor bekannter technologischer Zusammenhang sich unter gewissen Randbedingungen einstellen wird. Somit impliziert die Verwendung der Begriffe deduktiv und induktiv in Bezug auf die methodischen Suchstrategien zur Fehlermodellierung folglich keine unterschiedlichen Charakteristika hinsichtlich deren Eignung zur logischen Schlussfolgerung beziehungsweise deren Eignung zur probabilistischen Verwendung. Die Probabilistik, die diesen Methoden zugrunde liegt, ist jeweils dieselbe.

4 Rahmenkonzept für integrale Fehlermodelle

Die Methoden zur Fehleranalyse, -beschreibung und -bewertung technischer Systeme richten sich nach einem übergeordneten Verständnis, das auf einer Reihe von allgemeinen Annahmen, Anschauungen und Ansätzen zur formalisierten Beschreibung der betrachteten Systemeigenschaften beruht. Diese allgemeine Systematik der Fehlermodellierung bildet die Grundlage für die jeweils methodenspezifische Repräsentation der zu beschreibenden Systemcharakteristika und deren Auswertung. Als Grundlage für den integralen probabilistischen Ansatz zur Fehlermodellierung wird zunächst ein geeignetes Rahmenkonzept aus diesem übergeordneten Verständnis der methodischen Fehleranalytik abgeleitet.

4.1 Konzeptionelle Aspekte der methodischen Fehlermodellierung

Die rahmengebenden Konzepte der gebräuchlichen Ansätze der FMEA, FTA und RBD zur Beurteilung der Systemfunktionsfähigkeit anhand von Fehlermodellen bauen dabei auf drei gemeinsamen Grundelementen auf, dem der Struktur des Analyseobjekts, der Beurteilungskriterien und der Bewertungsmetrik.

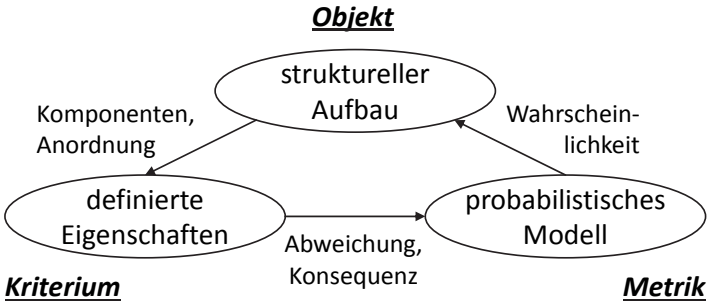


Bild 4.1: generalisierte Aspekte analytischer Methoden zur Fehlermodellierung

Wie in Bild 4.1 veranschaulicht ist, ist dies ist zum einen das Analyseobjekt, das typischerweise aus den einzelnen Systemkomponenten und deren struktureller Anordnung besteht. Die auf diese anzuwendenden Analysekriterien beruhen auf deren zweckdienlicher Weise vorgesehenen Eigenschaften und Verhaltensweisen der Komponenten als Einzelnes und im systemischen Zusammenspiel. Für die Fehleranalyse liegt der Fokus letztlich auf möglichen Abweichungen hiervon, sowie dadurch mögliche Konsequenzen und Effekte, typischerweise in Form von Ursache-Folge-Beziehungen. Der dritte Aspekt, der der Metrik, stellt die Maßgröße in Form der Wahrscheinlichkeit zur Bemessung der Möglichkeit der zu betrachtenden Vorgänge dar.

4.2 Differenzierung des methodischen Ansatzes gegenüber dem Stand der Technik

Das in dieser Arbeit thematisierte integrale Konzept der Fehlermodellierung wird nachfolgend anhand der drei konzeptionellen Aspekte, dem des strukturellen Aufbaus, dem der spezifizierten Eigenschaften und dem des probabilistischen Modells charakterisiert. Dazu erfolgt zunächst eine Differenzierung gegenüber den nach dem Stand der Technik bereits existierenden Ansätzen.

4.2.1 Systemstruktur

In technischen Systemen ist eine Betrachtung des strukturellen und funktionalen Systemaufbaus mittels einer mehrstufigen hierarchischen Untergliederung zweckmäßig und üblich [VDI-2206:04, Ehrlenspiel09]. Dies spiegelt sich unter anderem auch in methodischen Ansätzen zur Fehlermodellierung in der FTA [Vesely81], stärker ausgeprägt jedoch in RBD und FMEA mit Fehlernetzen [VDA-Band4-FMEA:06, DGQ-Band13-11:12] (nachfolgend: „FN-FMEA“) wider. Sinn und Prinzip der hierarchischen Ordnung des Fehlermodells ist dabei, die Fehlerbeziehungen grundlegend so aufzubauen, dass Fehlerursachen in Komponenten identifiziert und mit möglichen Auswirkungen im Kontext des Gesamtsystems in Bezug gesetzt werden (s. Kapitel 2). Dadurch wird der theoretische Ansatz umgesetzt, nach dem sich die Funktion eines Systems aus der geeigneten Funktion seiner Bestandteile ergibt und andernfalls fehlerhafte Eigenschaften aus Fehlern in dessen Bestandteilen hervorgehen.

4.2.2 Spezifikation

In enger Verbindung mit dem strukturellen Aspekt von Methoden steht der der angemessenen Spezifikation, woraus sich die Kriterien für Eignung oder Nichteignung von Eigenschaften ableiten. Dieser ist stets zumindest implizit die Grundlage aller Methoden der Fehlermodellierung. Am deutlichsten ist dies in der FMEA-Methode ausgeprägt, in der in einer systematischen Funktionsanalyse ausdrücklich identifiziert wird, welche Eigenschaften eine Komponente aufweisen muss, um anhand dessen ungeeignete Eigenschaften und Abweichungen definieren zu können. In der FTA geschieht dies überwiegend implizit, indem jeweils ein unerwünschtes Hauptereignis festgelegt wird und nach möglichen Ursachen dafür im System aufgrund von ungeeigneten Eigenschaften, Einwirkungen oder Konflikten im funktionalen Zusammenspiel gesucht wird. In RBD geschieht dies ebenfalls implizit und vergleichsweise weniger differenziert. Dies erfolgt, indem für Systembestandteile deren Funktionsfähigkeit beziehungsweise Ausfall als binäre Zustände pauschal definiert werden und eine Festlegung für das Erreichen des Ausfallzustands erfolgt. Im Ansatz der Mehrzustands-RBD erfolgt dies stärker differenziert in graduellen Abstufungen von Zustandsausprägungen. Aus diesen wird

mittels des probabilistischen Modells auf den allgemeinen Systemzustand in entsprechender binärer oder abgestufter Weise geschlossen.

Für die FTA ist nach [Vesely81] anhand technologisch-funktionaler Gesichtspunkte eine Einteilung in primäre, sekundäre und kommandierte Fehler zu beachten. Diese können darüber hinaus auch als Klassen probabilistischer Abhängigkeitsbeziehungen angesehen werden (s. Tabelle 4.1), die eine Randbedingung für die Vorgehensweise beim Aufbau eines Fehlermodells darstellen.

Tabelle 4.1: Fehlerkategorien nach [Vesely81]

	Definition der Fehlerkategorien	Probabilistische Abhängigkeit
Primärdefekt	ursächlicher Komponentendefekt in spezifikationsgemäßem Betrieb	unabhängig („zufällig")
Sekundärdefekt	Defekt durch Betrieb der Komponente ausserhalb deren Spezifikation	abhängig
Kommandierte Fehler	fehlerhaftes Verhalten von Komponenten ohne Defekt infolge fehlerhafter Ansteuerung	abhängig

4.2.3 Probabilistisches Modell

Die Auswertung des strukturhierarchischen Modells der FN-FMEA nach [VDA-Band4-FMEA:06, DGQ-Band13-11:12] ist nur auf qualitativer Basis definiert und bietet keine Grundlage zur gesamtheitlichen probabilistischen Auswertung des Systemverhaltens. Der Ansatz der Multiple-FMEA nach [Pickard05] stellt eine Interpretation der FMEA-Datenstrukturen im Stil einzelner Fehlerbäume dar, wird aber nicht grundlegend hinsichtlich probabilistischer Konsistenz diskutiert und fußt nicht auf einem Ansatz einer integralen Methodik. Vergleichbar verhält es sich mit der probFMEA nach [Kaiser15]. Die quantitativ definierte Methode der RBD beruht zwar auf einem vergleichbaren strukturhierarchischen Aufbau, ist jedoch primär auf Basis einer binären Fehlzustandsbetrachtung definiert. Daher werden hier keine verschiedenartigen Fehlzustände und Fehlerfolgen für das System differenziert. RBD-Ansätze zur Mehrzustands-Zuverlässigkeitsbewertung erweitern diese Möglichkeit innerhalb gewisser Grenzen. Dadurch sind zwar mehrere Fehlzustände je Systemteil definierbar, was aber im Rahmen von Abstufungen der allgemeinen Funktionsfähigkeit erfolgt. Dies bietet keine frei gestaltbare Möglichkeit, spezifische Zusammenhänge beliebiger Fehlzustände und deren Beziehung untereinander abzubilden. Ähnlich gilt dies für FTA und die Mehrzustands-FTA. So können dort spezifische Fehlzustandsdefinitionen festgelegt werden. Jedoch gilt für jeden Teilbaum jeweils ein konkretes Hauptereignis, gegebenenfalls in graduell abgestufter Zustandsausprä-

gung. Ferner ist die Möglichkeit zur systemhierarchisch ausgerichteten und probabilistisch konsistenten Modellierung zwischen verschiedenen Fehlerbäumen begrenzt.

Neben den klassischen Modellierungskonzepten sind insbesondere auch solche Ansätze relevant, die ein weiterentwickeltes Konzept der klassischen Fehlermodelle aufweisen. In [Lee02] wird ein Fehlermodell im Stil der FMEA mittels eines BN-Modells jeweils auf ein unerwünschtes funktionales Ereignis bezogen. Dies ist mit einem TOP-Level-Ereignis der FTA vergleichbar. In den Ansätzen der Component Fault Trees (CFT) [Kaiser03] und State-Event-Fault-Trees (SEFT) [Kaiser06] werden komplexe logische Strukturen genutzt, um das technologische Verhalten spezifischer Fehlerkomplexe durch die Systembestandteile sequenziell abzubilden. Hierbei ist im Modellierungskonzept kein gesamtheitlicher integraler Ansatz zur Systembeurteilung gegeben. In [Boissou03, Zhou06, Mi12, Zhai13, Cao16] werden Mehrzustands-Systemmodelle unter anderem mit mehrwertigen Zuständen in BN-Knoten berechnet, wobei dies jedoch aufgrund der Restriktion der RBD-Methodik und der Ansätze der Mehrzustands-Zuverlässigkeit nur begrenzte Möglichkeiten zur Darstellung verschiedenartiger Komponenten- und Systemzustände bietet.

Für die erläuterten Ansätze ist keine dedizierte Grundlage definiert beziehungsweise kein Prinzip im Modellierungsschema verankert, um ein gesamtheitliches System-Fehlermodell aufzubauen, in welchem unterschiedliche Komponenteneigenschaften und –zustände miteinander probabilistisch in Bezug stehen. Stattdessen werden spezifische Zusammenhänge vorrangig separat modelliert. Bei [Weber06] wird ein mögliches Gesamtschema anhand einer nach der SADT-Entwicklungsmethodik (aus dem Englischen: „Structured Analysis and Design Technique“, SADT) [Marca88, Ehrlenspiel09] systematisierten Anforderungs-und Funktionsstruktur aufgebaut. Es existiert hierbei jedoch nicht der Ansatz, einen systemisch ganzheitlichen und probabilistisch integralen Modellaufbau zu erzielen. Die Verfahren sind ferner nicht prinzipiell dahingehend ausgelegt, einzelne Teilsysteme verschiedener Detaillierungsebenen aufeinander aufbauend im hierarchischen Zusammenhang zu modellieren.

4.3 Definition eines strukturhierarchischen Grundkonzepts für integrale Fehlermodelle

Ausgehend von dem zuvor erläuterten methodischen Rahmenkonzept und der Differenzierung anhand des Stands der Technik kann ein Grundkonzept für ein integrales probabilistisches Fehlermodell eines Gesamtsystems beschrieben werden. Dies erfolgt wiederum anhand der zuvor diskutierten Kernaspekte des Rahmenkonzepts.

4.3.1 Festlegung des Konzepts bezüglich des Strukturmodells

In der Differenzierung gegenüber dem Stand der Technik wurde bereits verdeutlicht, dass die hierarchische Gliederung des Systems grundsätzlich bei der Fehlermodellierung zumindest in impliziter Weise Berücksichtigung findet. Für die FMEA-Fehlernetze finden diese sogar notwendigerweise ausdrücklich strukturgebend und systematisierend Anwendung. Auch für die FTA ist die systematische Betrachtung der hierarchischen Systemstruktur definiert, wenn auch nicht als obligatorischer Bestandteil des Grundprinzips. In RBD basieren sowohl das Analyseverfahren, als auch das Modellkonzept, sowie dessen wahrscheinlichkeitstheoretische Auswertung essentiell auf der gegebenen hierarchischen Systemstruktur. Eine an der Systemhierarchie ausgerichtete Analyse, ein danach aufgerichteter Aufbau der Fehlermodelle sowie deren probabilistische Auswertung sind wesentliche Bestandteile analytischer Methoden zur Fehleranalyse. Dies soll im Kontext dieser Arbeit hinsichtlich integraler Fehlermodelle daher sowohl richtungsweisend, als auch als verifizierte Herangehensweise zur Systembewertung gelten.

4.3.2 Definition des Konzepts zur Modellierung von Fehlzuständen

Für die Methodik zur gesamtheitlichen Fehlermodellierung dient ein an der Systemstruktur orientierter Aufbau des Fehlermodells, vergleichbar zum Prinzip der Fehlernetze der FN-FMEA. Nach diesem Schema gilt für das Modell, dass dieses analog zur Systemhierarchie abzuleiten ist. Daraus ergibt sich das Verständnis, dass Fehlzustände in Verbundkomponenten jeweils von den Fehlzuständen der Unterkomponenten abhängig modelliert werden.

Für Komponenten und Komponentenverbünde eines Systems beruht deren Funktion auf einer Anzahl definierter Eigenschaften, durch die sich der spezifizierte Produktbetrieb ergibt. Jegliche Abweichung von diesem Spezifikationsprofil stellt einen Fehlzustand dar. Folgt aus einer Abweichung kein relevanter Fehler, so stellt dies die betreffende Spezifikation grundsätzlich in Frage. Liegt mindestens ein Fehlzustand einer Komponente vor, befindet sich das System nicht im Zustand der uneingeschränkten Funktionsfähigkeit. Dies kann sich auf unterschiedliche Weise äußern, beispielsweise dem teilweisen oder völligen Ausfall des Systems beziehungsweise durch unerwünschte Verhaltensweisen.

Grundsätzlich wird angenommen, dass jeder Fehlzustand eines Bauteils zu einem Zeitpunkt einzeln vorliegen kann, nicht jedoch mehrere zugleich, sodass sie sich gegenseitig ausschließen. Auf dieser Annahme bauen Zuverlässigkeitsbetrachtungen nach dem allgemeinen Stand der Technik typischerweise auf, was auch im Rahmen dieser Arbeit als Randbedingung angenommen wird. Der Zustand einer Komponente, die gegebenenfalls aus mehreren Un-

terkomponenten besteht, ergibt sich aufgrund der Zustände der Unterkomponenten. Liegt in mindestens einer der Unterkomponenten ein Fehlzustand vor, so stellt dies einen spezifischen Fehlzustand des Verbunds dar (s. Bild 4.2). Verschiedene Konstellationen von Bauteilzuständen können vergleichbare Folgen für den Verbund bewirken und können als alternative Ursachen diesem jeweils zugeordnet werden.

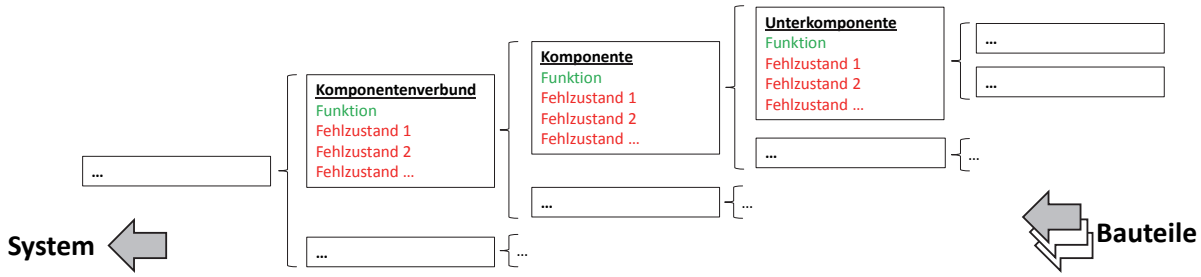


Bild 4.2: strukturhierarchisches Fehlermodell aus diskreten Zufallsvariablen

Die Soll-Funktionsweise einer Komponente stellt ein wichtiges Kriterium dar, um verschiedene Kategorien von Fehlzuständen zu unterscheiden. Für diese gelten jeweils unterschiedliche Charakteristika probabilistischer Abhängigkeiten, die deren Eingliederung in das Fehlermodell sowie die zugehörige Auswertung bestimmen, was im Laufe der Arbeit schrittweise konkretisiert wird.

4.3.3 Definition des Konzepts des probabilistischen Modells

Hinsichtlich des Grundverständnisses des probabilistischen Modells ist die hier gegebene Zielsetzung in wesentlichen Aspekten mit dem aussagenlogischen Grundverständnis in der FTA vergleichbar. Es werden logische Beziehungen zwischen Fehlerursachen und deren Folgen jeweils spezifisch zugeordnet, sowie auch Ursachenkombinationen, die neben möglichen alternativen Ursachen zur betreffenden Folge führen. Dies geschieht im Rahmen eines hierarchisch anhand des Systemaufbaus strukturierten Fehlermodells. Dies kann in gewissem Umfang mit dem Ansatz der FTA ebenso umgesetzt werden [Vesely81].

Jedoch kommen aufgrund des integralen Ansatzes weitere essentielle Aspekte für das probabilistische Modell hinzu. So bestehen Beziehungen zwischen den Zuständen von Komponenten mit beliebig vielen möglichen diskreten Zuständen auf mehreren Hierarchieebenen des Systems. Außerdem ist es im Rahmen integraler Fehlermodelle entscheidend, auch aufzeigen zu können, falls verschiedene Auswirkungen eines Fehlzustands alternativ eintreten können. Dies jedoch kann mittels bedingter Wahrscheinlichkeiten geschehen. Dies ist beispielsweise im Konzept der ETA in vergleichbarer Weise definiert. Eine probabilistische Grundlage zur entsprechenden Abbildung in Fehlermodellen existiert hierfür hingegen bis-

lang einzig in der probFMEA [Kaiser15]. Die Möglichkeit der Gestaltung eines solchen Ansatzes im Rahmen von BN-Modellen zeichnet sich in [Bobbio01, Kaiser06, Weber06, Khakzad11] bereits ab. Dort erfolgen jedoch keine grundlegende Herleitung sowie keine ausreichende Charakterisierung, insbesondere hinsichtlich kohärenter Fehlermodelle. In [Rauschenbach15] wurde dies thematisiert und dient als Ausgangspunkt für den in dieser Arbeit ausgeführten Ansatz. Die Differenzierung verschiedener möglicher Folgen ist jedoch ein wichtiges Merkmal für kohärente und integrale Fehlermodelle von Systemen. Dementsprechend zeigt sich dies in Fehlernetzen der FMEA, in welchen die Zuordnung mehrerer Folgen aus einer Fehlerursache genutzt wird. In der FMEA erfolgt dies in rein qualitativer Weise, ohne Differenzierung der damit verbundenen Häufigkeit. Eine probabilistische Auswertung kann jedoch eine umfassende Interpretation des Fehlermodells ermöglichen. So gilt dies beispielweise für Fälle, in welchen eine gegebene Ursache eine seltene kritische Folge haben kann oder aber eine andere, die häufiger folgt, dabei jedoch weniger kritische Auswirkungen erzeugt.

Die in Kapitel 4.2.2. erwähnte Kategorisierung von Fehlern nach [Vesely81] hat Einfluss auf die probabilistische Arithmetik, sodass dies bei der Fehlermodellierung gegebenenfalls geeignet berücksichtigt werden muss. Primäre Defekte sind solche Fehlzustände, die als unabhängige Fehlerursachen im Fehlermodell behandelt werden können. Diese sind solche Fehler, die in Bauteilen im Rahmen des spezifikationsgemäßen Betriebs in einer Komponente entstehen können. Sekundäre Defekte hingegen sind abhängig von der Wahrscheinlichkeit deren Ursache. Daher ist es günstigstenfalls näherungsweise korrekt, den Zustand der sekundär bettroffenen Komponente als unabhängigen Zufallswert abzubilden. Aus probabilistischer Sicht liegt hierbei jedoch eine bedingte Abhängigkeit des Konmponentendefekts vor. Sind mehrere Komponenten von diesen ungeeigneten Betriebsweisen oder –bedingungen betroffen, so sind diese zueinander bedingt unabhängig [Pearl00]. In dem Fall entwickeln sich die Fehlerfolgen jeweils voneinander unabhängig, während der ursächliche Fehler vorliegt (vgl. Kapitel 6.4). Die Ursache eines kommandierten Fehlers kann in einem Defekt einer anderen Komponente im System oder auch in einer Fehlerquelle ausserhalb des Systems liegen. Dies wiederum kann beispielsweise in Form einer fälschlichen Ansteuerung, einer unangeforderten Aktivierung zum betreffenden Zeitpunkt oder aber durch Ausbleiben einer erforderlichen Ansteuerung geschehen. Die jeweils fehlerhaft kommandierte Komponente jedoch erleidet dabei keinen Defekt, zeigt aber gegenüber ein ungeeignetes Verhalten verglichen mit der erwünschten Funktionsweise.

4.4 Zusammenfassung und Zwischenfazit

Durch die bisherige Eingrenzung des Rahmenkonzepts untergliedert sich das System der hierarchischen Struktur entsprechend in Unterkomponenten, die sich ihrerseits wiederum aus Unterkomponenten aufbauen. Für jede solche Komponente sind eine konkrete Anzahl möglicher Fehlzustände und ein Zustand der uneingeschränkten Funktionsfähigkeit definiert. Der vorherrschende Zustand der Komponente hängt von denjenigen der Unterkomponenten ab, die wiederum eine in sich geschlossene Einheit mit mehreren zueinander exklusiven Zuständen darstellen. Fehlzustände von Unterkomponenten werden den Zuständen des übergeordneten Verbunds logisch zugeordnet. Dies drückt aus, dass dies die Ursache für den jeweiligen Zustand oder gegebenenfalls mehrere ist.

5 Fehlzustandsbetrachtung mittels mehrwertiger diskreter Zufallsgrößen

Im vorigen Kapitel wurde ein Rahmenkonzept für das integrale Fehlermodell beschrieben, in dem unter anderem die Betrachtung der Systemkomponenten anhand mehrerer möglicher Zustände definiert wurde. Ziel des folgenden Abschnitts ist es, hierfür eine mengentheoretische und probabilistische Grundlage zur Behandlung mehrwertiger Zufallsgrößen zusammen zu stellen. Dies wird für eine Abbildung komplexer aussagenlogischer Beziehungen in integralen und kohärenten Fehlermodellen von Systemen benötigt.

5.1 Mengentheoretische Betrachtung des Schnitts mehrwertiger Zufallsgrößen

Vorbereitend wird zunächst eine geeignete probabilistische Anschauung des Zusammenspiels von Komponenten als Zufallsgrößen in Mengendiagrammen ausgeführt. Damit lässt sich ein zu den gebräuchlichen probabilistischen Termen für logische Operationen alternatives Berechnungsverfahren aufzeigen. Dieses beruht auf der Bildung aller kombinatorisch möglichen Schnittmengen und deren Rekombination zu logischen Aussagen. Das Schema eignet sich in besonderer Weise zur Veranschaulichung der logischen Beziehungen zwischen einzelnen Zuständen mehrwertiger Zufallsgrößen und dient im darauffolgenden Abschnitt als Grundlage für eine Methode zur Fehlermodellierung auf entsprechender Basis.

Für die in dem Themenbezug dieser Arbeit zu behandelnde Problemstellung sind Mengendiagramme trotz der im zweiten Kapitel erwähnten allgemeinen Einschränkungen zweckdienlich, da die logischen Verhältnismäßigkeiten im gegebenen Kontext fallweise schematisch beziehungsweise konkret bekannt sind. Diese dienen hierbei nicht als primäre Methode des Beweises beziehungsweise als alleiniges Argument für die Richtigkeit der Herangehensweise. Stattdessen verdeutlichen sie jedoch in schlüssiger Weise die Veranschaulichung der mengentheoretischen Grundlagen und charakteristischen logischen Zusammenhänge in Fehlerbeziehungen im System sowie deren Auswertung.

5.1.1 Grundlagen

In der verfügbaren Literatur zu methodischer Modellierung und Bewertung von Fehlerbeziehungen sowie der Zuverlässigkeit technischer Systeme wurden mengentheoretische Hintergründe vereinzelt bis zu einem gewissen Grad ausgeführt und veranschaulicht [DeLong70]. In [Vesely81] werden aussagenlogische Modelle aus einzelnen voneinander unabhängigen Fehlzuständen grundlegend erläutert. Zudem werden die Grundlagen der Theorie bedingter Wahrscheinlichkeiten im Kontext der Fehlermodellierung allgemein dargestellt, ebenso, wie auch die Theorie partitionierter Wahrscheinlichkeitsräume (s. Kapitel 2). Jedoch wurde deren

Umsetzung im Rahmen der methodischen Fehlermodellierung dort nicht aufgezeigt und seither auch an anderer Stelle offenbar nicht weiterverfolgt. Dies geschieht daher in diesem Abschnitt der Arbeit anhand grundsätzlicher mengentheoretischer Prinzipien. Wie nachfolgend gezeigt wird, lässt sich so ein umfassenderer Ansatz zur mengentheoretischen Darstellung formulieren. Aus dieser Anschauung ist die arithmetische Auswertung sich überlagernder mehrwertiger Zufallsgrößen systematisch nachvollziehbar. Dies wiederum ermöglicht die Veranschaulichung der mengentheoretischen Zusammenhänge zur Charakterisierung des im Zuge dieser Arbeit aufgebauten Modellierungskonzepts, was für dessen Definition genutzt wird.

In [Pfeiffer65, Vesely81] werden im Kontext der probabilistischen Fehleranalyse Darstellungen von Mengendiagrammen in Bezug auf den Wahrscheinlichkeitsraum im Rahmen der klassischen FTA angeführt und diskutiert. Dort finden auch die Prinzipien der totalen Wahrscheinlichkeit nach dem Kolmogorowschen Axiom des Einheitsraums $\boldsymbol{\Omega}$ mit der Mächtigkeit 1 in graphischer Darstellung als geschlossene umgebende Fläche von Mengendiagrammen Berücksichtigung. Weiter finden sich dort diverse Ausführungen unter anderem zu logischen Operationen, bedingten Wahrscheinlichkeiten, dem Bayes-Theorem und der Partitionierung von Mengen, jeweils im Kontext der probabilistischen Zusammenhänge in der methodischen Fehleranalyse.

In [Xizhi84] wird als Erweiterung der FTA-Methodik vorgeschlagen, die im Venn-Diagramm dargestellten Schnittmengen hinsichtlich der Eigenschaft der gegenseitigen Exklusivität soweit gegeben zusammenzufassen. Dies dient der Auswertung mehrerer Top-Level-Ereignisse verschiedener Fehlerbäume eines Systems in einer kombinierten Mehrzustands-Auswertung von Komponentenverbünden. Dabei jedoch werden kausale Zusammenhänge als Hintergründe der aussagenlogischen Verknüpfungen dieser zusammengefügten Top-Level-Ereignisse nicht näher erörtert.

5.1.2 Kontextbezogene Konventionen bezüglich mehrwertiger Zufallsgrößen

Im Hinblick auf die nachfolgenden Abschnitte und den Themenbezug der Arbeit wird der Index 0 als das Komplement der Verbundmenge A aus allen Partitionen zum universellen Wahrscheinlichkeitsraum $\boldsymbol{\Omega}$ definiert. In anderen Worten bedeutet dies, dass der Index 0 die Aussage „keine der in $\boldsymbol{A}$ enthaltenen Aussagen $\boldsymbol{A_i \neq 0}$ trifft zu" beziehungsweise in konkretem fachlichem Kontext „kein Fehlzustand liegt vor" repräsentiert. So gilt für die Zustandswahrscheinlichkeiten der mehrwertigen diskreten Zufallsgrößen aufgrund deren gegenseitiger Unvereinbarkeit (Exklusivität) und Komplementarität zur Wahrscheinlichkeit 1 (Exhaustivität):

$$\mathrm{P(A)} = \mathrm{P(a_0)} + \sum_{i \neq 0} P(a_i) = 1 \tag{5.01}$$

Im Hinblick auf Anschaulichkeit und unmittelbare Übertragbarkeit auf die nachfolgende methodische Verwendung wird eine Systematik der verwendeten Variablen mit Bezug auf den Kontext der Fehlermodellierung, wie in Tabelle 5.1 aufgeführt ist, definiert.

Tabelle 5.1: Systematik der verwendeten Variablen und Indizes in probabilistischem und fehleranalytischem Kontext

Variable	probabilistischer Kontext	fehleranalytischer Kontext
x_i $i \epsilon [0; n]$	Ereignis in probabilistischem Sinn; Feststellung des Ergebnisses eines Zufallsexperiments	Zustand im funktionalem Sinn (Funktionsfähigkeit bzw. Fehlzustand)
$X(x_i) =$ $x_0 \cup x_1 \cup \ldots \cup x_i \cup \ldots$ $\ldots \cup x_n$	Zufallsvariable, bezogen auf einen aussagenlogischen Gegenstand mit allen für diesen möglichen Aussagen x_i	Komponenten (z.B. Bauteile bzw. Bauteilverbünde, mit den für diese möglichen Zuständen)
x_0	Zustand des Nicht-Vorliegens der Klasse $x_{i \neq 0}$, also deren Komplements zur Gesamtwahrscheinlichkeit 1	Zustand der Abwesenheit jeglicher Fehlzustände
$X(x_{i \neq 0}) =$ $x_1 \cup x_2 \cup \ldots \cup x_i \cup \ldots$ $\ldots \cup x_n$	Klasse spezifischer Zustände des Gegenstands X	Gesamtheit aller möglichen Fehlzustände $x_{i \neq 0}$ einer Komponente X (z.B. eines Bauteils bzw. Bauteilverbunds)
$m_i n_j \ldots x_k$ $\widehat{=}$ $m_i \cap n_j \cap \ldots \cap x_k$	Tupel zur Symbolisierung des aussagenlogischen Zutreffens der Ereignisse m_i, n_j,..., x_k	Zustand des Vorliegens der Zustände m_i, n_j,..., $x_k$der Komponenten M, N, ..., X
Ω_X	Teil-Ergebnisraum des Betrachtungsrahmens bezüglich der Größe X unter Ausgrenzung evtl. weiterer Zufallsgrößen im universellen Wahrscheinlichkeitsraum Ω	probabilistischer Zustandsraum in Bezug auf eine isoliert betrachtete Komponente X
Ω_{XYZ}	Teil-Ergebnisraum des Betrachtungsrahmens hinsichtlich der Größen X, Y und Z	Verbund-Zustandsraum mit Betrachtungsrahmen bezogen auf die Komponenten X, Y und Z

Anhand dieser Nomenklatur wird im binären Fall eine Komponente A mit den Zuständen a_0 für deren fehlerfreie Funktionsfähigkeit und a_1 dem dazu gegenteiligen Fehlzustand deren Ausfalls eingestuft. In diesem binären Fall mit zwei Zuständen sind somit Funktionsfähigkeit

a_0 und Fehlzustand a_1 im Raum Ω_A zueinander komplementär und es gilt: $a_0 + a_1 = \Omega_A$. Der Teil-Ergebnisraum Ω_A der Komponente A unterteilt sich somit in zwei Klassen, der Funktionsfähigkeit a_0 und der Fehlzustände $a_{i\neq 0}$. Die Funktionsfähigkeit wird im Rahmen dieser Arbeit prinzipiell nicht weiter differenziert, sodass diese Klasse ausschließlich die Menge a_0 enthält. Die Klasse der Fehlzustände $a_{i\neq 0}$ besteht im binären Fall aus einer einzelnen Menge a_1 (vgl. Bild 5.1 links). Diese kann jedoch im Sinne der Mehrzustands-Zuverlässigkeit weiter untergliedert werden, sodass sich diese aus mehreren möglichen, sich gegenseitig ausschließenden Fehlzuständen, den Mengen $a_i \ni \{a_0, a_1, a_2, \dots\}$ zusammensetzt (s. Bild 5.1 rechts).

Bild 5.1: Repräsentation einer Komponente A im Teil-Ergebnisraum Ω_A als binäre Zufallsgröße (links) sowie als mehrwertige Zufallsgröße (rechts)

5.1.3 Überlagerung zweiwertiger diskreter Zufallsgrößen

In Darstellungen der grundlegenden Theorie bezüglich der Fehlermodellierung beispielsweise in [Watson62, Eckberg63, Barlow65, Vesely81] werden Schnitte unabhängiger Fehlzustände im System als Schnitt entsprechender Mengen innerhalb des universellen Ergebnisraums Ω dargestellt. Es ist wird dort jedoch nicht berücksichtigt, dass sich dabei nicht nur die Überlagerung der jeweiligen Fehlzustände ereignet. Die komplementären Zustände des Nicht-Vorliegens eines Fehlers sind dabei kombinatorisch ebenfalls existent. Solches wird entsprechend durch [Venn1880, Couturat1914] für die allgemeine Wahrscheinlichkeitstheorie gezeigt. Dort hingegen wird der Bezug zum Ergebnisraum Ω nach [Kolmogorow33] nicht berücksichtigt.

Berücksichtigt man jedoch beides bei der Überlagerung von Mengen, so sind sowohl die Schnitte mit den komplementären Mengen, als auch der endliche Ergebnisraum einzubeziehen. Dieser unterteilt sich dabei exhaustiv anhand aller kombinatorisch möglicher Schnitte dieser beiden Mengen und deren komplementärer Gegenmengen. Bei der Betrachtung des Schnitts voneinander stochastisch unabhängiger Zufallsgrößen A, B,… überlagern sich all deren Zustände in dem gemeinsamem Teil-Ergebnisraum $\Omega_{AB\dots}$. Dies ist in Bild 5.2 für drei zweiwertige Zufallsgrößen $A = \{a_0, a_1\}$, $B = \{b_0, b_1\}$ und $C = \{c_0, c_1\}$ dargestellt.

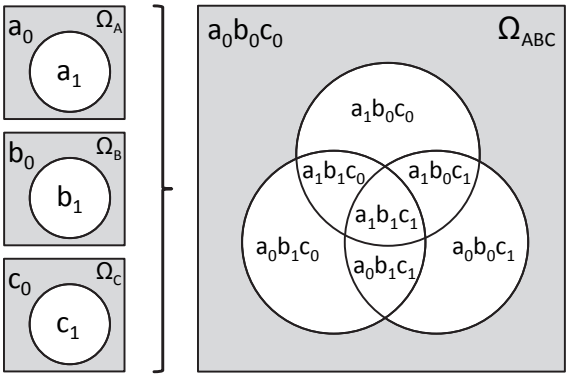


Bild 5.2: Venn-Diagramm dreier zweiwertiger Zufallsgrößen unter Berücksichtigung des Teil-Ergebnisraum $\boldsymbol{\Omega_{ABC}}$

5.1.4 Mengentheoretischer Schnitt mehrwertiger diskreter Zufallsgrößen

Im Rahmen der konzeptionellen Grundlage der Methodik zur Fehlermodellierung wurde die Betrachtung von Komponenten als diskrete Zufallsgrößen bereits zuvor als Annahme fixiert. So ergibt sich die Darstellung einer dreiwertigen Zufallsgröße in der zuvor getroffenen kontextspezifischen Konvention (s. Bild 5.3) analog zu der Theorie partitionierter Mengen [Pfeiffer65, Vesely81]. Die jeweiligen Zustände einer diskreten Zufallsgröße sind zueinander komplementär und gegenüber $\boldsymbol{\Omega}$ exhaustiv. Sie schneiden sich untereinander nicht und sind stattdessen unvereinbar.

Bei der Überlagerung der Zufallsgrößen $A = \{a_0, a_1, \dots, a_i, \dots, a_p\}$, $B = \{b_0, b_1, \dots, b_j, \dots, b_{qq}\}$ und $C = \{c_0, c_1, \dots, c_k, \dots, c_r\}$ können alle Ergebniskombinationen in Form von elementaren Mengenschnitten (Mintermen) der Überlagerungs- beziehungsweise Verbundzustände auftreten. Die untereinander exklusiven Tupel $a_i b_j c_k$ repräsentieren dabei jeweils eine der möglichen Zustandskombinationen $a_i \cap b_j \cap c_k$ für alle $i \in [0; p]$, $j \in [0; q]$ und $k \in [0; r]$ des Verbunds ABC als elementare Schnittmengen.

$$\begin{aligned} \Omega_{ABC} &= A \cup B \cup C = \bigcup_{i,j,k} \{a_i \cap b_j \cap c_k\} \\ &= a_0 b_0 c_0 \cup a_1 b_0 c_0 \cup a_0 b_1 c_0 \cup a_0 b_0 c_1 \cup a_1 b_1 c_0 \cup a_1 b_0 c_1 \cup a_0 b_1 c_1 \cup a_1 b_1 c_1 \end{aligned} \tag{5.02}$$

Im Folgenden gelte $a_i b_j c_k$ als vereinfachte Schreibweise für $a_i \cap b_j \cap c_k$ nach [Peano1888] (vgl. auch Tabelle 5.1), ebenso wie $P(a_i b_j c_k)$ für $P(a_i \cap b_j \cap c_k)$.

Die Darstellung nach Bild 5.2 kann nach der zuvor festgelegten Indizierungskonvention im Sinne der Fehlzustandsbetrachtung eines Verbunds aus den Komponenten A, B und C gedeutet werden. Dabei steht der Index 0 für die Aussage „$funktionsfähig$" beziehungsweise der Index 1 für „$ausgefallen$". Beispielsweise bezeichnet die elementare Schnittmenge $a_1 b_0 c_0$

beispielsweise den Zustand, in dem A ausgefallen ist, während B und C zugleich uneingeschränkt funktionsfähig sind. Für die Überlagerung im gemeinsamen Ergebnisraum werden ebenfalls die Klassen der Funktionsfähigkeit und des Fehlzustands in Bezug auf den Verbund definiert. Funktionsfähigkeit des Verbunds ist gegeben, wenn alle enthaltenen Größen den Index 0 aufweisen, was der Zustandskombination $a_0 b_0$ entspricht (s. Bild 5.3).

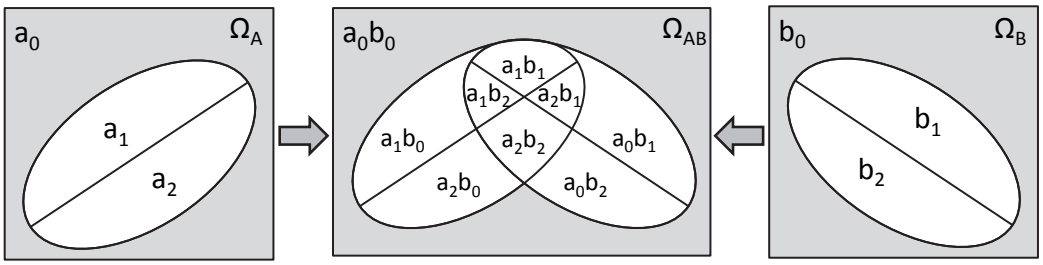


Bild 5.3: Schnitt zweier Zufallsvariablen (A, B) mit je zwei exklusiven Zuständen

Das Darstellungsschema in Bild 5.3 ist dabei mit Blick auf den thematischen Hintergrund der Arbeit gewählt. Aufgrund des spezifischen Verständnisses, dass es jeweils einen Zustand des Nichtvorliegens und einen beziehungsweise mehrere des Vorliegens von Fehlzuständen gibt. So können in einem anderen Kontext unterschiedliche Mengengruppierungen sinnfällig sein oder die Gruppierung unterbleiben, was den allgemeingültigen Fall darstellt. Dies jedoch ist letztlich eine Frage der Veranschaulichung jeweils identischer Inhalte.

In Anbetracht der zuvor dargestellten Zusammenhänge stellt die Interpretation mehrwertiger Zufallsgrößen keine grundlegende Erweiterung gegenüber dem Fall binärer Zufallsgrößen dar. Stattdessen handelt es sich vielmehr um deren Übertragung auf ein erweitertes Feld kombinatorischer Möglichkeiten innerhalb der gebräuchlichen theoretischen Anschauung. Die Eigenschaften der Exklusivität und exhaustiven Komplementarität gelten gleichermaßen für solche mit beliebig vielen gegenseitig exklusiven Zuständen, wie sie auch für zweiwertige Zufallsgrößen zutreffend sind. Allgemein gilt dabei für die Überlagerung $\{AB \ldots\}$ der diskreten mehrwertigen und exhaustiven Zufallsgrößen A, B,… :

$$A \cup B \cup \ldots = \bigcup_{i,j,\ldots} [a_i \cap b_j \cap \ldots] = \Omega_{AB\ldots} \tag{5.03}$$

Mit diesem Schema können aussagenlogische Beziehungen bei Schnitten mehrwertiger Zufallsgrößen miteinander systematisch dargestellt werden. Dies wird nachfolgend dazu verwendet, allgemeine probabilistische Grundgleichungen in Bezug auf mehrwertige Zufallsgrößen herzuleiten. Dies wiederum wird im darauffolgenden Kapitel als Basis für die arithmetische Auswertung probabilistisch integraler Fehlermodelle verwendet.

Die Menge aus allen Zustandskombinationen, in welchen mindestens eine der beteiligten Größen einen Fehlzustand mit $i \neq 0$ repräsentiert, ist die Klasse der Fehlzustände des Verbunds. Diese lässt sich anhand der Anzahl n der in der Zustandskombination repräsentierten Fehlzustände in verschiedene Gruppen einteilen, wovon meist Fehlzustände der ersten und vereinzelt der zweiten Ordnung aus probabilistischer Sicht von vorrangigem Interesse sind:

- uneingeschränkte Funktionsfähigkeit: Zustandskombination des Verbunds, in welchem *keine* der sich darin überlagernden Komponenten einen Fehlzustand aufweisen (in obigem Beispiel $a_0 b_0$).
- Fehlzustand erster Ordnung (Einfachfehler): Zustandskombinationen in welchen jeweils *genau eine* der sich im Verbund überlagernden Komponentenzustände einen Fehlzustand aufweist (z.B. $a_1 b_0$, $a_0 b_1$, $a_2 b_0$ und $a_0 b_2$)
- Fehlzustand zweiter Ordnung (Doppelfehler): Zustandskombinationen, in welchen jeweils *genau zwei* der sich im Verbund überlagernden Komponentenzustände einen Fehlzustand aufweisen (z.B. $a_1 b_1$, $a_2 b_1$, $a_1 b_2, a_2 b_2$)
- Fehlzustand n-ter Ordnung: Zustandskombinationen, in welchen jeweils *genau* n der sich im Verbund überlagernden Komponentenzustände einen Fehlzustand aufweisen
- Fehlzustand höherer Ordnung (als n): Zustandskombinationen, in welchen jeweils *mehr als* n der sich im Verbund überlagernden Komponentenzustände einen Fehlzustand aufweisen (z.B. in Bezug auf n=2 für alle Fehlerkombinationen oberhalb der Ordnung von Doppelfehlern)

5.2 Probabilistische Auswertung der Überlagerung mehrwertiger Zufallsgrößen

Im voranstehenden Abschnitt erfolgte eine Herleitung der mengentheoretischen Zusammenhänge durch die Zusammenführung des Konzepts des Wahrscheinlichkeitsraums und der vollständigen kombinatorischen Berücksichtigung des Schnitts partitionierter Mengen in diesem. Das dabei entstandene Schema erlaubt die Darstellung und aussagenlogische Interpretation mehrwertiger Zufallsgrößen in deren Überlagerung in Mengendiagrammen. Nach [Kolmogorow33] können solchen mengentheoretischen Beziehungen Wahrscheinlichkeitsmaße zugeordnet und auf Basis aussagenlogischer Beziehungen ausgewertet werden (vgl. Kapitel 2). Im folgenden Abschnitt wird anhand dessen gezeigt, dass diese kombinatorische Betrachtungsweise die aussagenlogisch-probabilistische Auswertung mehrwertiger Zufallsgrößen erlaubt.

5.2.1 Grundlagen

Nach dem grundlegend anerkannten Stand der Wissenschaft, lässt sich eine logische Aussage A als Teilmenge des universellen Ergebnisraum Ω darstellen, welcher nach der Axiomatik Kolmogorows die totale Wahrscheinlichkeit $P(\Omega) = 1$ hat. Dem Zutreffen der Aussage A, respektive der Menge A wird ein Wahrscheinlichkeitsmaß $0 \leq P(A) \leq 1$ zugeordnet. Der Bereich des Ergebnisraums komplementär zu A ist dessen Gegenereignis A^c :

$$A \cup A^c = \Omega \tag{5.04}$$

$$P(A) + P(A^c) = P(A \cup A^c) = P(\Omega) = 1 \tag{5.05}$$

In [Vesely81] werden unter anderem Schnitte einer einzelnen Menge mit dem in Teilmengen partitionierten Wahrscheinlichkeitsraum behandelt. Dieser partitionierte Wahrscheinlichkeitsraum wird als eine Menge behandelt. In den folgenden Termen dieses Teilabschnitts wird vorübergehend der Skritptbuchstabe $\mathcal{A}$ für diese verwendet, um die Exhaustivität dieser partitionierten Menge über den gesamten Wahrscheinlichkeitsraum zu kennzeichnen. Dies ist in den sich daran anschließenden Abschnitten kontextbedingt nicht mehr nötig, sodass die nachfolgenden Ausführungen wieder ausschließlich nach der festgelegten Nomenklatur in Tabelle 5.1 im Abschnitt 5.1.2 ausgerichtet sind.

So besteht die Menge $\mathcal{A}$ aus den Teilmengen a_1, a_2, … a_n (s. Bild 2.3, rechts), die sich jeweils einander gegenseitig ausschließen und aussagenlogisch betrachtet, sich gegenseitig ausschließende Aussagen repräsentieren. Die Menge $\mathcal{A}$ erstreckt sich über den gesamten Ergebnisraum, was hier als exhaustiv bezeichnet wird. Für eine solche partitionierte exhaustive Menge $\mathcal{A}$ gilt:

logisch: $$\bigcup_i(a_i) = a_1 \cup a_2 \cup \ldots \cup a_i \cup \ldots \cup a_n = \mathcal{A} = \Omega \quad \text{sowie} \tag{5.06}$$

$$\bigcap_i(a_n) = a_1 \cap a_2 \cap \ldots \cap a_i \cap \ldots \cap a_n = \{\} \tag{5.07}$$

probabilistisch: $$P(\bigcup_i(a_i)) = P(a_1 \cup a_2 \cup \ldots \cup a_i \cup \ldots \cup a_n) = P(\mathcal{A}) = 1 \tag{5.08}$$

$$P(\bigcap_i(a_n)) = P(a_1 \cap a_2 \cap \ldots \cap a_i \cap \ldots \cap a_n) = 0 \tag{5.09}$$

Die Zufallsvariable $\mathcal{A} \ni \{a_1, a_2, \ldots, a_i, \ldots, a_n\}$ enthält alle den Partitionen $i \in \{0,1,2, \ldots, i, \ldots, n\}$ jeweils zukommende Aussagen. Der Wahrscheinlichkeitsvektor $P(\mathcal{A})$ beinhaltet deren jeweilige Wahrscheinlichkeit. Dabei sind die Zufallsgröße und deren Wahrscheinlichkeitsvektor exhaustiv, sodass dessen gesamte Wahrscheinlichkeit der totalen Wahrscheinlichkeit entspricht. Diese ergibt sich aus der arithmetischen Summe der einzelnen Zustandswahrscheinlichkeiten, da diese gegenseitig exklusiv sind.

$$P(\mathcal{A}) = \begin{bmatrix} P(a_1) \\ P(a_2) \\ \dots \\ P(a_i) \\ \dots \\ P(a_n) \end{bmatrix} = \sum_i P(a_i) = 1 \tag{5.10}$$

In [Vesely81] wird gezeigt, wie sich die Zustände a_i einer exhaustiven Zufallsgröße jeweils im Schnitt mit einer einzelnen probabilistisch verhalten (vgl. Bild 2.3 rechts). Demnach gilt als universelle Gleichung für den Schnitt einer exhaustiven Menge $\mathcal{A}$ aus Partitionen a_i mit einer singulären Menge B auf Grundlage bedingter Wahrscheinlichkeiten:

$$P(\mathcal{A} \cap B) \;=\; P(B|\mathcal{A}) \cdot P(\mathcal{A}) \;=\; P(\mathcal{A}|B) \cdot P(B) \tag{5.11}$$

Sind $\mathcal{A}$ und B voneinander unabhängig, so gilt $P(\mathcal{A}|B) = P(\mathcal{A})$ sowie $P(B|\mathcal{A}) = P(B)$ und aus (5.08) wird damit die Produktregel für den Schnitt der exhaustiven partitionierten Menge $\mathcal{A}$ mit der von dieser unabhängigen Wahrscheinlichkeitsgröße B:

$$P(\mathcal{A} \cap B) = P(\mathcal{A}) \;\cdot P(B) \tag{5.12}$$

Sind $\mathcal{A}$ und B gegenseitig exklusiv, ist $P(\mathcal{A} \cap B) = 0$ beziehungsweise $(\mathcal{A} \cap B) = \{\}$, da deren Schnittmenge leer ist und es gilt $P(B|\mathcal{A}) = 0$ sowie $P(\mathcal{A}|B) = 0$. Für den Schnitt von n exhaustiven Partitionen a_i , $i = [1, \dots k, \dots n]$ mit einer Menge B gilt nach [Vesely81] unter der Bedingung, dass $\mathsf{U}_i(a_i) = \Omega$ und $P\{\mathsf{U}_i(a_i)\} = 1$ sind:

$$P(B \cap a_i) \;=\; P(B|a_i) \cdot P(a_i) \;=\; P(a_i|B) \cdot P(B) \tag{5.13}$$

$$P(B) \;=\; P\left\{\bigcup\nolimits_i (B \cap a_i)\right\} \;=\; \sum\nolimits_i P(B \cap a_i) \;=\; \sum\nolimits_i \{P(B|a_i) \cdot P(a_i)\} \tag{5.14}$$

Die Wahrscheinlichkeit der Vereinigungsmenge entspricht der Summe der einzelnen Wahrscheinlichkeiten, da sich die Partitionen gegenseitig nicht schneiden. Aus (5.13) und (5.14) leitet sich nach [Vesely81, Krieg01] das Bayessche Theorem für Partitionen des Ergebnisraums ab:

$$P(a_k|B) = \frac{P(B|a_k)P(a_k)}{\sum_i P(B|a_i)P(a_i)} \tag{5.15}$$

Sind A und B jeweils probabilistisch abhängig von einer weiteren Größe C, gilt ferner für das allgemeine Bayes-Theorem [Russell95]:

$$P(A|B,C) = \frac{P(B|A,C)P(A|C)}{P(B|C)} \tag{5.16}$$

5.2.2 Wahrscheinlichkeiten elementarer Schnitte unabhängiger diskreter Zufallsgrößen

Die im vorigen Abschnitt wiedergegebene Herleitung der Wahrscheinlichkeit der Schnittmenge diskreter Partitionen mit einer einzelnen unabhängigen Menge nach [Vesely81] lässt sich auf den Fall sich überlagernder mehrwertiger diskreter Zufallsgrößen ausweiten. Dazu kann man sich zunächst anhand der zuvor diskutierten mengentheoretisch integralen Betrachtungsweise vergegenwärtigen, dass die Gleichungen (5.13) und (5.14) in analoger Weise auf B^c, das Komplement von B, zutreffen. Ersetzt man darin das Ereignis B durch B^c, beschreiben diese schließlich den Schnitt einer Partition a_i mit dem Gegenereignis B^c. B und B^c verhalten sich dabei zueinander ebenso, wie die Partitionen von A. Daraus lässt sich folgern, dass die Gleichungen auf den allgemeinen Fall zweier sich überlagernder exhaustiver Partitionen a_i, $i = [0,1,\dots n]$ und b_j, $j = [0,1,\dots m]$ übertragen werden können. Daher gilt analog zu (5.13) beziehungsweise (5.14):

$$P(b_j \cap a_i) = P(b_j|a_i) \cdot P(a_i) = P(a_i|b_j) \cdot P(b_j) \tag{5.17}$$

$$P(b_j) = P\{\cup_i (b_j \cap a_i)\} = \sum_i P(b_j \cap a_i) = \sum_i P(b_j|a_i) \cdot P(a_i) \tag{5.18}$$

Gleichung (5.17) findet sich auch in [Pearl82] in Bezug auf Inferenznetzwerke mit Zufallsgrößen beliebiger diskreter Wahrscheinlichkeitsverteilung. Mit (5.17) und (5.18) ist das Bayessche Theorem in Bezug auf zwei exhaustive partitionierte Zufallsgrößen:

$$P(a_k|b_j) = \frac{P(b_j|a_k)P(a_k)}{\sum_i P(b_j|a_i)P(a_i)} \tag{5.19}$$

Dabei ist für unabhängige Zufallsgrößen A und B: $P(B|A) = P(B)$:

$$P(b_j|a_i) = P(b_j) \quad \text{bzw.} \quad P(b_j|a_k) = P(b_j) \tag{5.20}$$

Da aufgrund der Exhaustivität $\Sigma_i P(a_i) = 1$ gilt, ergibt sich aus (5.19):

$$\Sigma_i P(b_j|a_i) \cdot P(a_i) = P(b_j) \cdot \Sigma_i P(a_i) = P(b_j) \tag{5.21}$$

Letztlich ist:

$$P(a_k|b_j) = P(a_k) \tag{5.22}$$

In Bezug auf mehrere Zufallsgrößen gilt hierbei nach Gleichung (2.10):

$$P(a_i \cap b_j \cap c_k \cap \dots) = P(a_i) \cdot P(b_j|a_i) \cdot P(c_k|a_i \cap b_j) \tag{5.23}$$

Sind A, B, C, … unabhängig, gilt nach (5.22) $P(b_j|a_i) = P(b_j)$, $P(c_k|a_i \cap b_j) = P(c_k)$, … usw.

Dies bedeutet, dass auch für die Wahrscheinlichkeit $P(a_i b_j \dots)$, dem Schnitt der Partitionen a_i, b_j, … der unabhängigen Zufallsgrößen A, B,… mit jeweils exhaustiven Wahrscheinlichkeitsverteilungen gilt:

$$P(a_i b_j \dots) = P(a_i \cap b_j \cap \dots) = P(a_i) \cdot P(b_j) \cdot \dots \tag{5.24}$$

Somit gilt auch die Produktregel unabhängiger Wahrscheinlichkeiten für die jeweiligen elementaren Schnittmengen $a_i b_j \dots$ aller im Ergebnisraum $\Omega_{A,B,\dots}$ möglichen Zustandskombinationen der unabhängigen exhaustiven sowie diskreten mehrwertigen Zufallsgrößen A, B,… . Da diese elementaren Schnittmengen zudem gegenseitig exklusiv sind, erfolgt deren Disjunktion miteinander zu Verbundmengen durch arithmetische Addition deren Wahrscheinlichkeiten. Mit Bezug auf Abschnitt 5.1 und Gleichung (5.02) gilt daher allgemein für die Gesamtwahrscheinlichkeit der Disjunktion zweier unabhängiger, mehrwertiger, diskreter und exhaustiver Zufallsgrößen grundsätzlich:

$$\begin{aligned} P(A \cup B \cup \dots) &= P\left[\bigcup_{i,j,k,\dots} [a_i \cap b_j \cap \dots]\right] \\ &= \sum_{i,j,\dots} [P(a_i)P(b_j) \dots] = P(\Omega_{AB\dots}) = 1 \end{aligned} \tag{5.25}$$

5.2.3 Bedingte Unabhängigkeit

Sind Zustände b_j und c_k verschiedener Zufallsgrößen B beziehungsweise C nicht unmittelbar voneinander abhängig, werden jeweils jedoch durch dieselbe Wahrscheinlichkeit a_i bedingt, so werden diese als bedingt unabhängig bezeichnet [Pearl82]. Dies veranschaulicht das Beispielsschema in Bild 5.4. $P(b_j|a_i)$ und $P(c_k|a_i)$ sind darin jeweils von der Wahrscheinlichkeit $P(a_i)$ abhängig. Gegenseitig beeinflussen sich diese jedoch nicht unmittelbar, sodass sie innerhalb des Rahmens der gemeinsamen Bedingtheit durch A untereinander unabhängig sind.

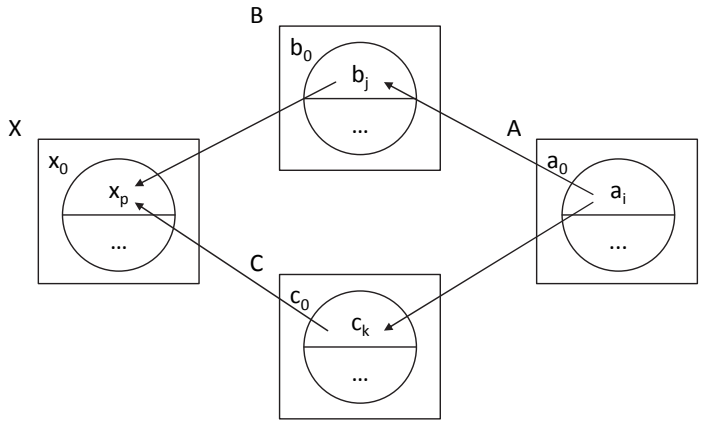


Bild 5.4: Zufallsgröße X in Abhängigkeit von bedingt unabhängigen Zufallsgrößen B und C

Angenommen, der Zustand x_p der diskreten Zufallsgröße X hängt ab von der Konjunktion der Zustände b_j und c_k der Zufallsgrößen B und C, die wiederum beide von demselben Zustand a_i abhängen (s. Bild 5.4). So gilt auf Basis des Bayes-Theorems nach Gleichung (2.05) und dessen Anwendung auf die Kombination mehrerer Größen anhand von (2.10) hierfür:

$$\begin{aligned} P(x_p) = P(c_k \cap b_j) = {} & P(c_k|b_j) \cdot P(b_j) \\ = {} & P[(c_k|a_i)|(b_j|a_i)] \cdot P(a_i) \cdot P(b_j|a_i) \cdot P(a_i) \end{aligned} \tag{5.26}$$

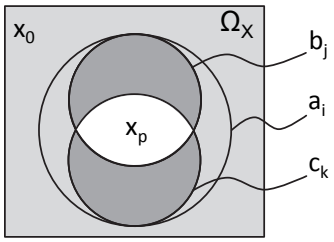


Bild 5.5: Zustand x_p als Schnittmenge der in Abhängigkeit von a_i bedingt unabhängigen Zustände b_j und c_k.

Nach dem Bayes-Theorem in der auf partitionierte Ergebnisräume bezogenen Form nach (5.19) gilt:

$$\begin{aligned} P\big[(c_k|a_i) \mid (b_j|a_i)\big] &= \frac{P[(b_j|a_i) \mid (c_k|a_i)] \ \cdot \ P(c_k|a_i)}{\sum_n P\big[(b_j|a_i) \mid (c_n|a_i)\big] \cdot P(c_n|a_i)} \\ &= \frac{P(b_j|a_i) \ \cdot \ P(c_k|a_i)}{P(b_j|a_i) \ \cdot \ \sum_n P(c_n|a_i)} = \frac{P(c_k|a_i)}{P(a_i)} \end{aligned} \tag{5.27}$$

Aufgrund der bedingten Unabhängigkeit von B und C ist darin:

$$P\big[(b_j|a_i) \mid (c_k|a_i)\big] = P(b_j|a_i). \tag{5.28}$$

A und C sind exhaustive Zufallsgrößen sodass analog zu Gleichung (5.14) die Summe aller deren Schnitte ebenfalls exhaustiv ist

$$\sum_n P(c_n|a_i) = \sum_n P(c_n)P(a_i) \;=\; P(a_i) \tag{5.29}$$

Somit ergibt sich aus dem Bayes-Theorem für bedingt unabhängige Zustände:

$$\begin{aligned} P(x_p) &= \frac{P(c_k|a_i)}{P(a_i)} P(a_i) \cdot P(b_j|a_i) \cdot P(a_i) \\ &= P(c_k|a_i) \cdot P(b_j|a_i) \cdot P(a_i) \end{aligned} \tag{5.30}$$

Demnach gilt im Fall der Disjunktion zweier bedingt unabhängiger diskreter Zufallsgrößen für die arithmetische Betrachtung einzelner Zustände a_i und deren Wahrscheinlichkeiten:

$$\begin{aligned} P(x_p) &= P(c_k \cap b_j) = P(c_k|a_i)\, P(a_i) \cdot P(b_j|a_i) P(a_i) \\ &= P(c_k|a_i) \cdot P(b_j|a_i) \cdot P(a_i) \end{aligned} \tag{5.31}$$

Die letzte Umformung beruht auf dem Idempotenzgesetz (Tabelle 2.1 (3)) nach den Axiomen des Logikkalküls [Peano1888]. Deren Anwendbarkeit auf die Überlagerung diskreter Zufallsgrößen wird im nachfolgenden Kapitel anhand der Beziehungen in integralen Fehlermodellen eingehend dargestellt. Zugunsten von Anschaulichkeit und Anwendungsorientierung der Betrachtungen wird auf einen universellen formalen Beweis, wie bereits im einleitenden Kapitel erwähnt, verzichtet. Die Schlüssigkeit der Zusammenhänge sowie die Übereinstimmung mit den im nachfolgenden Kapitel 6 ausgeführten Rechenbeispielen werden als hinreichende Verifikation im Sinne der Zielsetzung erachtet.

5.2.4 Bedingte Wahrscheinlichkeit möglicher Folgen

Anstelle der zuvor behandelten Verwendung ausschließlich ein-eindeutiger gerichteter logischer Beziehungen zwischen Mengen kann die Zuordnung der Zustände mehrwertiger Zufallsgrößen nach [Pearl82, Kim83] jedoch auf Basis bedingter Wahrscheinlichkeiten geschehen, um Ungewissheit in logischen Beziehungen abbilden zu können. Dies lässt sich mit dem Bayesschen Theorem in Gleichung (2.05) behandeln. In Kapitel 5.2.2 wurde dessen Anwendung auf die Beziehung zwischen den diskreten Zuständen voneinander abhängiger Zufallsgrößen betrachtet. In diesem Zusammenhang können bedingte Wahrscheinlichkeiten beliebige Werte annehmen, solange $\Sigma_\xi P(x_\xi|a_i b_j \dots) = 1$ sowie $0 \leq P(x_\xi|a_i b_j \dots) \leq 1$ erfüllt sind.

Gilt für einen Zustand x_j der Zufallsgröße X, dass diese mit einer Wahrscheinlichkeit $0 < P(x_j|a_i)P(a_i) < 1$ auf einen Zustand a_i folgt, dann ist nach Gleichung (5.17):

$$P(x_j) = \frac{P(x_j|a_i)}{P(a_i|x_j)} P(a_i) \tag{5.32}$$

Ist in einem speziellen Fall a_i die einzige gegebene Einflussgröße, durch die x_i bedingt wird, so gilt im Umkehrschluss immer dann a_i={‚$wahr$'}, wenn es zutrifft, dass x_i={‚$wahr$'} ist und zugleich x_i gilt. In diesem Fall ist $P(a_i|x_j) = 1$. Gilt dabei jedoch umgekehrt, dass x_i nicht zwangsläufig zutrifft wenn a_i={‚$wahr$'} ist, sondern lediglich in einem Anteil der Fälle, dann drückt $P(x_j|a_i)$ die Möglichkeit des jedoch ungewissen Eintretens von a_i aus für den Fall, dass a_i zutrifft (vgl. auch Kapitel 2.4). In diesem spezifischen Zusammenhang gilt:

$$P(x_j) = \frac{P(x_j|a_i)}{P(a_i|x_j)} = P(x_j|a_i)P(a_i), \qquad \text{für } P(a_i|x_j) = 1 \tag{5.33}$$

Diese Zuordnung von Anteilen der Menge a_i zu a_i für $j \neq 1$ ist in Bild 5.6 symbolisiert.

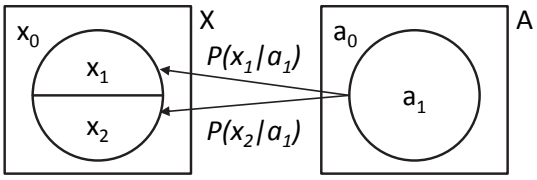


Bild 5.6: Partitionierung in alternativ mögliche Ereignismengen bei Ungewissheit der Folge

Dieser spezielle Fall entspricht der typischen Fragestellung bei der methodischen Fehleranalyse, in dem verschiedene Folgen einer Ursache möglich sind. Aufgrund des Zwecks der Untersuchung wird dabei typischerweise betrachtet, zu welcher Folge eine Ursache, sei es ein einzelner Fehler oder eine Fehlerkombination, möglicherweise führt. Solch ein anteiliger Einfluss eines ursächlichen Zustands a_i auf die Folge x_i, wird im Folgenden mit der spezifischen Schreibweise angegeben:

$$P(x_j|a_i) = \delta_{a_i \to x_j} \tag{5.34}$$

Intuitiv interpretiert ist $\delta_{a_i \to x_j} = 0$ der Fall, wenn keine Möglichkeit besteht, dass diese Folge eintritt, $0 < \delta_{a_i \to x_j} < 1$, wenn in einem entsprechenden Teil der Fälle die Möglichkeit besteht, dass diese Folge eintreten kann. Im Fall $\delta_{a_i \to x_j} = 1$ gilt, dass die Folge mit gleicher Wahrscheinlichkeit, wie deren Ursache zutrifft.

Nach [Pearl82] drücken solchen Beziehungen in BN eine probabilistische Ungewissheit im Sinn der subjektivistischen Wahrscheinlichkeitsauffassung aus. Nach [Pearl00, Jaynes03] jedoch können die subjektivistische und objektivistische Auffassung als Teilsichten einer allgemeiner gefassten Wahrscheinlichkeitsauffassung betrachtet werden (s. Kapitel 2.1.3). Pearl bezieht sich jedoch auf Ungewissheit bezüglich der Hypothese, die die Inferenz bedingt. Dementgegen wird hier jedoch nicht die Wahrscheinlichkeit des Zutreffens von Hypothesen modelliert, sondern faktisch mögliche Kausalbeziehungen. Diese werden im Kontext der Fehlermodellierung jedoch als bekannt vorausgesetzt (vgl. Kapitel 3.3.1). Die Ungewissheit besteht stattdessen in der diskreten Häufigkeitsverteilung im frequentistischen Sinn. Demnach würde sich dieser Zusammenhang bei theoretisch unendlicher Anzahl von Fällen des ursächlichen Ereignisses einstellen.

Die Betrachtung möglicher alternativer Folgeereignisse ist dabei kongruent zum probabilistischen Konzept in der technischen Systemzuverlässigkeit, das im Sinne von [Chorafas60] als Ersatzmodell für das Verhalten deterministischer physikalischer Zusammenhänge angewendet wird (vgl. Kapitel 2.2). Im Folgenden wird diese bedingte Wahrscheinlichkeit zur Abbildung von Möglichkeiten des Ausgangs im Zuge der Wahrscheinlichkeitsauswertung daher zur Auswertung von Folgewahrscheinlichkeiten im Fall gegebener Ursachen verwendet. In diesem Zusammenhang sei

$$P\big(Folge\ x_j\big) \;=\; \delta_{a_i \to x_j} \cdot P(Ursache\ a_i)$$

definiert als der bedingt wahrscheinliche beziehungsweise mögliche Beitrag der Ursache $\boldsymbol{a_i}$ zur Wahrscheinlichkeit der Folge $\boldsymbol{x_i}$. In [MIL-1629A:80, DIN-25419:85, Kaiser06, Kaiser15] wurde dies in ähnlicher Weise bereits vorgeschlagen. Dies erfolgte jedoch nicht in einem entsprechenden probabilistischen Zusammenhang für Mehrzustands-Zufallsgrößen und zudem nicht im Kontext eines integralen Fehlermodells eines Systems. Ferner wurde diese bedingte Folgewahrscheinlichkeit bereits in [Bobbio01, Lee02, Weber06, Khakzad11] implizit genutzt, jedoch ohne dies auf die hier gezeigte arithmetische Grundlage und den thematischen Kontext zu beziehen. Dies wird in Kapitel 6.1.2 und den darauffolgenden Ausführungen im Rahmen der Fehlermodellierung weitergeführt.

Anschaulich ausgedrückt teilen die bedingten Folgewahrscheinlichkeiten die ursächlichen Mengen in zueinander komplementäre Anteile auf, nach dem Prinzip der Partitionierung von Mengen. Im gegebenen Fall kann deren Behandlung in probabilistischer Hinsicht in Analogie zu den zuvor beschriebenen probabilistischen Schemata erfolgen. Zur Erhaltung der probabilistischen Integrität und Konsistenz eines Gesamt-Fehlermodells eines Systems müssen diese im hier behandelten integralen Schema vollständig und eindeutig zugeordnet werden. Al-

le klassischen Methoden wie FTA und RBD verwenden dabei stets implizit die totale Wahrscheinlichkeit, indem stets angenommen wird, dass die Folge eintritt, sobald die Ursache vorliegt. Die Werte für $\delta_{a_i \to x_j} \in [0,1]$ stellen dagegen eine proportionale Zuordnung dar:

$$P\begin{pmatrix} x_0 \\ x_1 \\ x_j \\ \dots \end{pmatrix} = \begin{pmatrix} \delta_{a_i \to x_0} \\ \delta_{a_i \to x_1} \\ \delta_{a_i \to x_j} \\ \dots \end{pmatrix} \cdot P(a_i) \tag{5.35}$$

Dies kann intuitiv auch als prozentualer Ausdruck der probabilistischen Möglichkeit (übersetzt aus dem Englischen „likelihood") unterschiedlicher Folgen interpretiert werden. Die Aussage einer solchen differenzierten Beziehung der Folgewahrscheinlichkeit kann folgendermaßen umschrieben werden:

Liegt der Fehlzustand a_i vor, dann folgen:

- x_0 in $(\delta_{a_i \to x_0}) \cdot 100\,\%$ der Fälle
- x_1 in $(\delta_{a_i \to x_1}) \cdot 100\,\%$ der Fälle
- x_j in $(\delta_{a_i \to x_j}) \cdot 100\,\%$ der Fälle
- ...

5.3 Aussagenlogische Projektion mehrwertiger Zufallsgrößen in Verbundmengen

Auf Basis von logischen Zuordnungen zwischen Mengen können Aussagen in der Form „wenn A gilt, dann trifft auch B zu" dargestellt werden. Dies ermöglicht auch die probabilistische Interpretation, indem die Wahrscheinlichkeit der Ausgangsmenge A mittels der logischen Beziehung auf B projiziert wird. Im folgenden Unterabschnitt wird dies in Bezug auf mehrwertig diskrete Zufallsgrößen in einem integralen Konzept angewendet. Dies geschieht zudem unter Berücksichtigung der zuvor betrachteten Konstellationen probabilistischer Abhängigkeiten. Ausgehend von den Betrachtungen und Herleitungen in den vorigen Teilabschnitten kann dies mit einem systematischen und verhältnismäßig unkomplizierten arithmetischen Schema geschehen.

5.3.1 Grundlagen

Nach dem Stand von Wissenschaft und Technik werden Aussagewahrscheinlichkeiten im Kontext logischer Operationen üblicherweise mit den Gleichungen (2.06) und (2.07) berechnet. Das dahinterliegende Verständnis ist, dass die Mächtigkeit der gesuchten Ergebnismenge aus geeigneter Addition, Subtraktion und Multiplikation der durch den Schnitt erzeugten Teilmengen bestimmbar ist. Die durch die Zerlegung in elementare Teilmengen repräsen-

tierten Aussagen können so interpretiert werden, dass der gemeinsame Bereich $A \cap B$ der Aussage „A und zugleich B" entspricht, die beiden anderen hingegen bedeuten „A ohne B" (symbolisch: $A \backslash B$) beziehungsweise „B ohne A" (symbolisch: $A \backslash B$) (s. Bild 5.7). Die durch den Schnitt erzeugten Teilmengen repräsentieren eine jeweils spezifische Aussage.

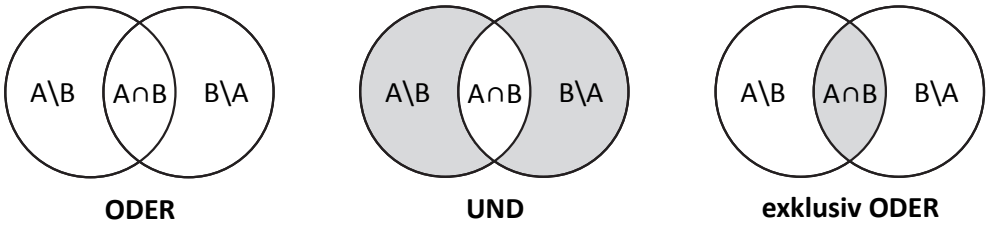


Bild 5.7: Darstellung logischer Operationen auf Basis exklusiver Schnittmengen

5.3.2 Logische Operationen auf Basis der Zustände mehrwertiger Zufallsgrößen

Ausgehend von der in Kapitel 5.1 erörterten Überlagerung mehrwertiger Zufallsgrößen unter Berücksichtigung aller möglichen Zustände in einem gemeinsamen Verbundraum lassen sich diese Schnitte auch unmittelbar aus den Disjunktionen der Partitionsmengen bestimmen (vgl. Bild 5.8). Aussagenlogisch entsprechen diese den elementaren Schnittmengen.

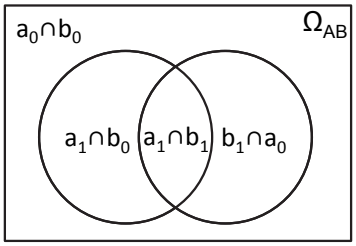


Bild 5.8: elementare Teilmengen des Schnitts mehrwertiger Zufallsgrößen

Das Prinzip ist unabhängig von der Anzahl der überlagerten Zufallsgrößen und deren Zustände. Betrachtet man den Fall zweier sich schneidender zweiwertiger Zufallsgrößen so entspricht beispielsweise $a_1 \backslash b_1$ der Schnittmenge $a_1 \cap b_0$, da b_0 und b_1 zueinander komplementär sind. Analog gilt dies für $b_1 \backslash a_1$. Demnach lassen sich logische Aussagen als Schnittmengen der Partitionen der Teil-Wahrscheinlichkeitsräume Ω_A und Ω_B im Verbundraum Ω_{AB} auffassen. Für die logischen Operationen gilt daher alternativ zu (2.06), (2.07) und (2.08):

$$P(a_1 \cap b_1) = P(a_1)P(b_1) \tag{5.36}$$

$$P(a_1 \cup b_1) = P(a_1)P(b_0) + P(a_0)P(b_1) + P(a_1)P(b_1) \tag{5.37}$$

$$P(a_1 \underline{\cup} b_1) = P(a_1)P(b_0) + P(a_0)P(b_1) \tag{5.38}$$

Diese aussagenlogischen Operationen können auch vektoriell dargestellt werden:

$$P(a_1 \cap b_1) = [0 \quad 0 \quad 0 \quad 1] \begin{bmatrix} P(a_0) \cdot P(b_0) \\ P(a_1) \cdot P(b_0) \\ P(a_0) \cdot P(b_1) \\ P(a_1) \cdot P(b_1) \end{bmatrix} \tag{5.39}$$

$$P(a_1 \cup b_1) = [0 \quad 1 \quad 1 \quad 1] \begin{bmatrix} P(a_0) \cdot P(b_0) \\ P(a_1) \cdot P(b_0) \\ P(a_0) \cdot P(b_1) \\ P(a_1) \cdot P(b_1) \end{bmatrix} \tag{5.40}$$

$$P(a_1 \underline{\cup} b_1) = [0 \quad 1 \quad 1 \quad 0] \begin{bmatrix} P(a_0) \cdot P(b_0) \\ P(a_1) \cdot P(b_0) \\ P(a_0) \cdot P(b_1) \\ P(a_1) \cdot P(b_1) \end{bmatrix} \tag{5.41}$$

Verallgemeinert gilt hierbei, dass aussagenlogische Operationen prinzipiell aus der integralen Überlagerung mehrwertiger diskreter Zufallsgrößen mittels Bildung der elementaren Schnittmengen und deren geeigneter Addition umsetzbar sind. Anhand der mengentheoretischen Herleitung des Überlagerungsschemas gilt dies analog für die Überlagerung beliebig vieler Zufallsgrößen mit jeweils beliebig vielen diskreten Zuständen, wobei eine explizite Darstellbarkeit aufgrund der Zahl möglicher Kombinationen jedoch gewissen Grenzen unterliegt.

5.3.3 Kohärente Aussagenlogik und Arithmetik mehrwertiger Zufallsgrößen

Für mehrwertige Variablen mit mehr als jeweils zwei sich gegenseitig ausschließenden diskreten Zuständen ist das zuvor behandelte Prinzip analog anwendbar. So gelte beispielsweise im Fall zweier sich schneidender Zufallsvariablen $A \ni [a_0, a_1]$ und $B \ni [b_0, b_1, b_2]$ (s. Bild 5.9), für eine Wahrscheinlichkeit $P(x_1)$ einer Ergebnisvariablen X:

$$P(x_1|A,B) = \mathrm{P}(\mathrm{a}_1 \cup \mathrm{b}_2) = P(a_1)P(b_0) + P(a_1)P(b_2) + P(a_0)P(b_2) \tag{5.42}$$

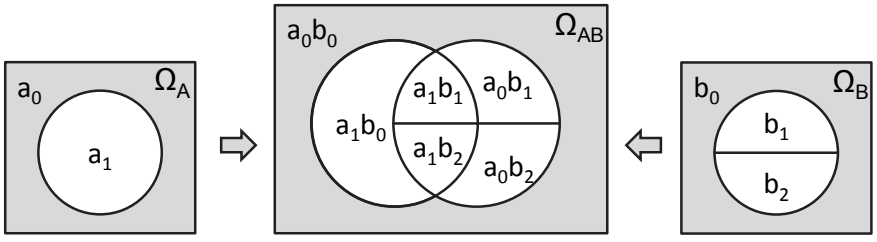


Bild 5.9: Überlagerung der diskreten Zufallsgrößen A und B im Verbundraum Ω_{AB}

Die Kombination $a_1 \cup b_2$ entspricht der inklusiven Konjunktion (logisches ODER) zwischen den Zuständen $a_1$und $b_2$der Variablen A und B. Stehen diese Zustände im Fall eines probabilistischen Fehlermodells jeweils für einen konkreten Fehlzustand der Komponenten A beziehungsweise B, so gilt für $x_1 = a_1 \cup b_2$ die Aussage, dass der Zustand x_1 des Komponentenverbunds X vorliegt, wenn a_1 oder b_2 beziehungsweise beide zugleich vorliegen.

Die Zufallsgrößen sind in den Darstellungen dieses Abschnitts grundsätzlich so veranschaulicht, dass die Zustandsindizes $i \neq 0$ die jeweils möglichen Abweichungen vom Ausgangszustand, also der Funktionsfähigkeit, repräsentieren. Zustände mit Index 0 und ebenso Konjunktionen ausschließlich aus solchen mit Index 0 repräsentieren dabei den Zustand des Nicht-Vorliegens jeglicher Abweichung vom Ausgangszustand, also der uneingeschränkten Funktionsfähigkeit. Dabei ist zu beachten, dass bei sich gegenseitig ausschließenden Teilmengen a_i und a_j einer Zufallsgröße A deren Schnitt einer leeren Menge entspricht $a_i \cap a_j = \{\}$. Die Wahrscheinlichkeit deren Konjunktion ist folglich $P(a_i) \cdot P(a_j) = 0$.

Diese in Bild 5.9 dargestellten Schnittmengen sollen in einem Beispiel den Partitionen x_0, x_1 und x_2 der Zufallsgröße X, wie in Bild 5.10 veranschaulicht ist, zugeordnet werden.

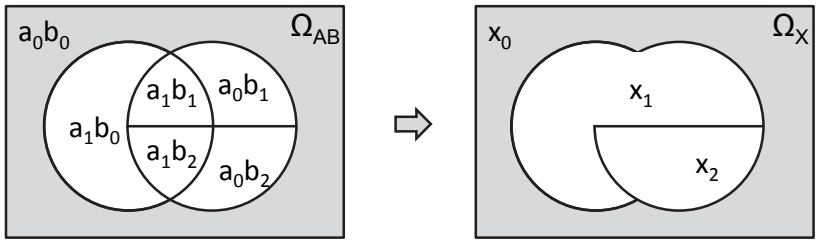


Bild 5.10: Zuordnung der Schnittmengen der Partitionen der Zufallsgrößen A und B zu Partitionen der Größe X

Diese Zuordnung aller in Ω_{AB} kombinatorisch möglichen Schnittmengen zu den Werten x_i der Zufallsgröße X kann in Form eines konsistenten Gleichungssystems ausgedrückt werden:

$$P(x_0) = P(a_0 \cap b_0) = P(a_0)P(b_0) \tag{5.43}$$

$$P(x_1) = P(a_1 \cup b_1) = P(a_0)P(b_1) + P(a_1)P(b_0) + P(a_1)P(b_1) \tag{5.44}$$

$$P(x_2) = P(b_2 \underline{\cup} (a_1 \cap b_2)) = P(a_0)P(b_2) + P(a_1)P(b_2) \tag{5.45}$$

Diese logischen Beziehungen lassen sich durch mehrere logische Graphen in Anlehnung an Fehlerbäume symbolisieren (s. Bild 5.11). Aufgrund des oben für dieses Beispiel veranschaulichten integralen Beziehungsschemas sind die drei logischen Graphen dabei komplementär zum gesamten Ergebnisraum Ω_X. Dies bedeutet, dass sich diese gegenseitig exhaustiv zur

totalen Wahrscheinlichkeit ergänzen. Die Zustände $a_{i\neq 0}$, $b_{i\neq 0}$ und $x_{i\neq 0}$ darin sind jeweils zueinander exklusiv, was insbesondere für die Eindeutigkeit der Auswertung relevant ist und im gegeben Fall konkret den Zustand b_2 betrifft. Wie in Gleichung (5.45) bereits umgesetzt wurde, weswegen $P(b_2) = P(b_2 \backslash a_{i\neq 0}) = P(a_0) \cdot P(b_2)$ ist.

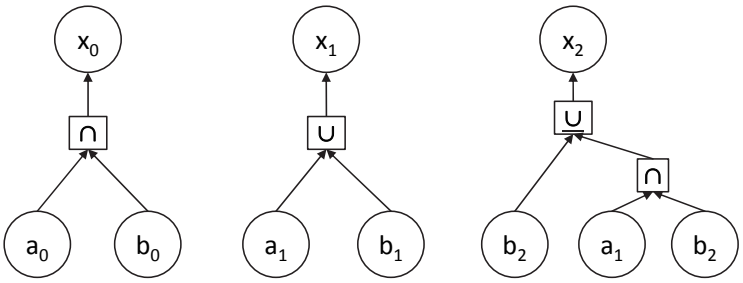


Bild 5.11: logische Beziehungsstrukturen zwischen einzelnen Größen der Eltern- und Kindvariablen im integralen Netzwerkmodell in Anlehnung an Fehlerbäume

Bild 5.12 symbolisiert die Überlagerung der Variablen A und B in Ω_{AB}, deren Gruppierung zu Verbundmengen x_i mit jeweils gleichartigen logischen Aussagen und die dazu umzusetzende Arithmetik. Die Visualisierung ist analog zu dem Prinzip nach [Darwiche02] und ähnlich zur Darstellung der Sum-Product Networks nach [Poon11].

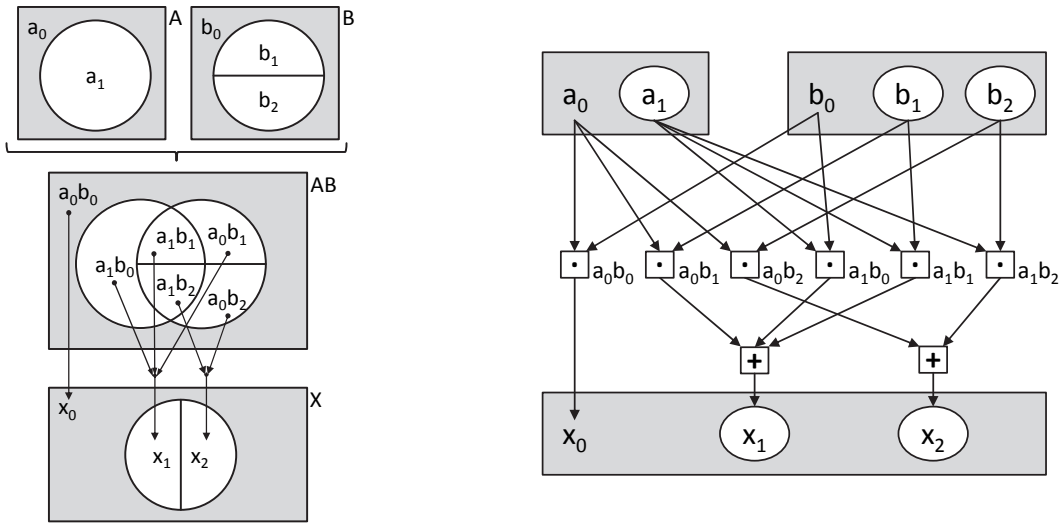


Bild 5.12: Veranschaulichung des Schnitts mehrwertiger Zufallsvariablen A und B als Mengendiagramm (links), sowie als arithmetisches Schema (rechts).

Jedoch bestehen inhaltliche Unterschiede hinsichtlich der Systematik deren Aufbaus, aufgrund anderer Zielsetzungen der Auswertung im dort geltenden Kontext. Zudem bezieht sich das in [Poon11] behandelte Schema ausschließlich auf die Kombination jeweils zweier zweiwertiger Variablen. Das hier beschriebene Schema gilt prinzipiell für beliebig viele unbeschränkt mehrwertige Variablen. Gleichwohl jedoch unterliegt die graphische Veranschauli-

chung jedoch Restriktionen in Bezug auf deren Nachvollziehbarkeit. Daher wurde die Anzahl an Variablen und deren Zustände im Beispiel aus Gründen der Übersichtlichkeit vergleichsweise gering gehalten.

5.4 Zusammenfassung und Zwischenfazit

Zusammenfassend gilt somit, dass sich die Wahrscheinlichkeit der jeweiligen elementaren Schnittmengen aus dem Produkt aller sich überlagernder Partitionen ergibt. Die Kombination der Wahrscheinlichkeiten der elementaren Schnittmengen zur Wahrscheinlichkeit des Folgezustands entspricht der arithmetischen Summe der Wahrscheinlichkeitswerte, da die Zustände gegenseitig exklusiv sind. Unterteilungen von Mengen in Partitionen werden in gleicher Weise als einzelne exklusive Mengen analog zu den Eingangszuständen der Zufallsgrößen gehandhabt. Dabei stellen die jeweiligen Konstellationen spezifische aussagenlogische Operationen dar. So lassen sich durch arithmetisches Zuordnen der Wahrscheinlichkeiten zutreffender elementarer Schnittmengen zu Folgezuständen Ursache und Folgebeziehungen probabilistisch ausdrücken. Gemeinsame Abhängigkeiten lassen sich anhand des Bayes-Theorems analytisch erfassen und berechnen.

Anhand dieses Schemas und der darin nachvollziehbaren logischen Operationen ist eine aussagenlogische Interpretation probabilistisch integraler Fehlermodelle möglich. Dies geschieht im nachfolgenden Kapitel am Beispiel von BN-Fehlermodellen, die auf dem untersuchten arithmetischen Schema beruhen. Dazu soll dieses bewährte probabilistische Verfahren als Berechnungswerkzeug zur Untersuchung derartiger Fehlermodelle und darin auftauchender stochastischen Problemstellungen genutzt werden.

6 Fehlzustandsmodelle mit mehrwertigen Zufallsgrößen

Nachdem im vorigen Kapitel grundlegende probabilistische Schemen der Überlagerung mehrwertiger Zufallsgrößen und deren arithmetische Ausdrücke charakterisiert wurden, ist es das Ziel für dieses Kapitel, deren Anwendung im Kontext der methodischen Fehlermodellierung zu untersuchen und zu verifizieren. Dazu wird gezeigt, dass diese in BN-Modellen auf entsprechende Weise umsetzbar sind. Ein solcher Nachweis existiert bislang nicht in der erforderlichen Betrachtungstiefe und Durchgängigkeit. Dies erlaubt anschließend deren Nutzung zur Zuverlässigkeitsbewertung technischer Systeme in einer Differenzierbarkeit der Zustände, wie dies bislang im Stand von Wissenschaft und Technik nicht gegeben ist. In der Umsetzung ermöglicht dies eine tiefergehende und differenziertere aussagenlogische Fehlermodellierung mit BN.

Zu einzelnen Aspekten der methodischen Umsetzung von Fehlerbeziehungen technischer Systeme in BN-Modellen existieren bereits einige unmittelbar oder indirekt zutreffende Arbeiten, in welchen die darin umgesetzten aussagenlogischen Zusammenhänge jedoch nicht in erschöpfendem Maß erörtert werden. Anhand des probabilistischen Prinzips von BN und den verfügbaren Ansätzen zu deren Nutzung zur Zuverlässigkeitsbewertung wird nachfolgend gezeigt, welche aussagenlogischen und probabilistischen Beziehungen zwischen einzelnen Zuständen sich beeinflussender Zufallsgrößen konkret darstellbar sind. Grundlage hierfür sind die vorangegangenen allgemeinen aussagenlogischen Überlegungen bezüglich der Überlagerung mehrwertiger Zufallsvariablen. Unter anderem erfolgen dazu eine Verifikation der zuvor analytisch aufgezeigten probabilistischen Zusammenhänge sowie die anwendungsorientierte Umsetzung in komplexen Fehlermodellen. Die geschieht durch die Berechnung der jeweils im Kontext dargestellten BN-Modellen innerhalb der verwendeten Softwareumgebung [GeNIe10] auf Grundlage des exakten Clustering-Algorithmus [Lauritzen88].

6.1 Grundlagen probabilistischer Netzwerke auf Basis mehrwertiger Zufallsgrößen

Die Inferenz in BN beruht nach [Pearl82] auf Familien von logischen Beziehungen in der Art von „Wenn x_i … dann …y_j“. Konkrete Zusammenhänge, Veranschaulichungen oder Interpretationen dieser Beziehungen zwischen einzelnen Zuständen der Zufallsvariablen wurden bislang jedoch nicht spezifisch betrachtet. Dies ist aus Sicht von Pearl [Pearl82] und Kim [Kim83] nicht von Bedeutung, da das Augenmerk aufgrund des dort gegebenen fachlichen Hintergrunds der künstlichen Intelligenz und der statistischen Datenanalyse nicht auf der detaillierten Charakterisierung und gezielten Darstellung einzelner mengentheoretischer Operationen liegt. Analog dazu schreibt [Charniak91] bezüglich der Berechnungsverfahren solcher Netz-

werke, dass der Berechnungsalgorithmus bereits für einfache unverzweigte Baumgraphen kompliziert sei, weswegen dieser dort nicht erläutert werde. Dies trifft entsprechend stärker auf komplexere Graphentopologien zu. Pearl nennt als Grundlagen zur Berechnung der BN allgemein das Bayes-Theorem und eine Normalisierungskonstante [Pearl82, Kim83, Pearl85], ohne deren mathematischen Hintergrund und deren Bestimmung näher darzustellen. [Russell95] erläutert diese als Normalisierung des berechneten Wahrscheinlichkeitswerts des Zustands der jeweils einzelnen Größen durch die Summe der Wahrscheinlichkeiten aller resultierenden Zustände, sodass die Summe der Wahrscheinlichkeiten der totalen Wahrscheinlichkeit mit dem Wert 1 entspricht. So gelangt [Lampis09] im Kontext der Fehlermodellierung mit BN zu der Einschätzung, dass die konkreten Vorgänge bei der Berechnung der Netzwerke im Verborgenen liegen. Einzig in [Darwiche02, Poon11] wird in kontextspezifischer Umsetzung für je zwei zweiwertige Variablen ein Ansatz zur aussagenlogischen Interpretation einzelner Inferenzbeziehungen von Eltern- und Kindknoten betrachtet (s. Kapitel 5.3.3).

6.1.1 Fehlermodellierung in BN

[Bobbio01, Lee02, Boissou03, Weber06, Lampis09, Zhai13, Cao16] zeigen Ansätze, um BN für quantitative Fehleranalysen in unterschiedlichen Stilen zu nutzen, jedoch ohne die aussagenlogischen Zusammenhänge grundlegend und im zuvor dargestellten systemischen Gesamtzusammenhang zu differenzieren. So können durch die Wahrscheinlichkeiten von Folgezuständen im Sinn logischer Aussagen durch geeignetes Zuordnen der Zustandskombinationen in den CPT implementiert werden. Die Schemen der CPT für ein ODER- beziehungsweise ein UND-Gatter sind in den Tabellen 6.1 und 6.2 dargestellt.

Tabelle 6.1: CPT zur Abbildung eines ODER-Gatters in BN

A		wahr		falsch	
B		wahr	falsch	wahr	falsch
X	wahr	1	1	1	0
	falsch	0	0	0	1

Tabelle 6.2: CPT zur Abbildung eines UND-Gatters in BN

A		wahr		falsch	
B		wahr	falsch	wahr	falsch
X	wahr	1	0	0	0
	falsch	0	1	1	1

Ein Gatter für eine zwei aus drei Mehrheitsentscheidung (2:3-Gatter) kann nach [Bobbio01] in CPT gemäß Tabelle 6.3 ausgedrückt werden.

Tabelle 6.3: CPT zur Abbildung eines 2:3-Gatters in BN

A		wahr				falsch			
B		wahr		falsch		wahr		falsch	
C		wahr	falsch	wahr	falsch	wahr	falsch	wahr	falsch
X	wahr	1	1	1	0	1	0	0	0
	falsch	0	0	0	1	0	1	1	1

In [Lampis09] werden ferner NICHT-Gatter in analoger Weise implementiert. Ferner wurden Gatter der dynamischen FTA in dynamischen BN umgesetzt [Weber03, Montani05]. Die konkreten arithmetischen Zusammenhänge und probabilistische Abhängigkeiten einzelner Zustände wurden jedoch nicht eingehend untersucht. Ein analytischer Nachweis der in den bisherigen Werken empirisch gehandhabten logischen Zusammenhänge ist bislang nicht verfügbar. Daher soll die arithmetische Grundlage nachfolgend explizit untersucht werden, um deren spezifischen Charakteristika explizit nachweisen und diese zur integralen Fehlermodellierung unter Berücksichtigung probabilistischer Abhängigkeiten für beliebige Modellkomplexe nutzen zu können.

Für ein differenziertes Mehrzustands-Zuverlässigkeitsmodell dagegen sind mehrere Zustände der Komponenten in jeweils einem Knoten zusammenhängend abzubilden. Beispielsweise in [Portinale99, Bobbio01, Portinale15] wurde die in BN gegebene Möglichkeit zur Verwendung von Mehrzustands-Variablen in dem Kontext der Fehleranalyse grundsätzlich erwähnt, jedoch ohne deren Umsetzung im Hinblick auf die Fehlermodellierung im Detail zu behandeln. So erfolgte keine nähere Untersuchung hinsichtlich der dabei zu behandelnden Kombinatorik beziehungsweise der zugrundeliegenden Arithmetik und der darzustellenden aussagenlogischen Beziehungen. Auch in [Khakzad11] ist ein Beispiel eines Mehrzustands-Ansatzes verfügbar, für das die probabilistischen Zusammenhänge jedoch nicht thematisiert wurden. Nachfolgend wird daher eine Modellierung auf Basis mehrwertiger Zufallsgrößen ausführlich dargestellt und bezüglich ihrer Charakteristika näher untersucht. Dies bildet die Grundlage für das Ziel, ein Konzept zur integralen probabilistischen Fehlermodellierung aufstellen zu können.

Auch das Strukturierungsschema zum Aufbau der Netzwerkmodelle ist ein essentieller Aspekt im Sinne der Problemstellung. Nach dem gebräuchlichen Aufbau werden für jeweils abzubildende logische Operationen jeweils separate BN-Knoten verwendet, wie unter anderem in [Portinale99, Bobbio01, Lee02, Weber03, Lampis09]. Dadurch kann es je nach Umfang des Systemabbildes mitunter problematisch sein, komplexe Systemstrukturen in einem Modell dieses Prinzips zu bewerten. Je nach Grad der Detaillierung sind nach diesem vorherrschen-

den Strukturierungsschema erhebliche Anzahlen an Knoten umzusetzen, sodass die Netzwerke sehr umfangreich und komplex werden können. Neben der Aufwandsbewältigung ist dabei fraglich, ob Konsistenz und Nachvollziehbarkeit eines System-Fehlermodells gewährleistet werden können.

6.1.2 Probabilistische Ungewissheit anhand bedingter Wahrscheinlichkeiten

Bei der Erarbeitung von Fehlernetzen in der FN-FMEA [VDA-Band4-FMEA:06, DGQ-Band13-11:12] werden unterschiedliche Folgen eines Fehlzustands einer Komponente in qualitativer Weise identifiziert. Die FMECA erlaubt eine Differenzierung verschiedener Folgewahrscheinlichkeiten für eine jeweils gegebene Fehlerursache [MIL-1629A:80]. Gleiches gilt für die ETA in Bezug auf Ereignissequenzen. In probabilistischen Ursache-Folge-Beziehungen ist es mitunter bedeutsam, Ungewissheit des Ausgangs solcher Folgebeziehungen differenziert darstellen zu können, da so eine Unterscheidung angesichts der Wahrscheinlichkeit beispielsweise besonders relevanter Folgen differenziert werden kann. In den bisher veröffentlichten Ansätzen zur Fehlermodellierung in BN wurde die Möglichkeit der Nutzung differenzierter bedingter Wahrscheinlichkeiten zur Darstellung unterschiedlicher möglicher Folgezustände nur in begrenztem Umfang aufgezeigt. In [Lee02] wird allgemein vorgeschlagen, alternative Fehlerfolgen in der BN-FMEA zu modellieren. [Bobbio01, Khakzad11] erwähnen die Möglichkeit der Darstellung ungewisser Folgen in BN-Fehlermodellen vor dem methodischen Hintergrund der FTA. Die einzelnen probabilistischen Zusammenhänge wurden jeweils nicht spezifisch und nicht unter generellen methodischen Gesichtspunkten diskutiert.

Nach der Definition von BN [Pearl82] kann Ungewissheit in BN durch bedingte Wahrscheinlichkeiten in das probabilistische Modell einbezogen werden. Dies wurde in Kapitel 5.2.4 bereits grundlegend diskutiert. Nachfolgend wird dies hinsichtlich der methodischen Verwendung auf Mehrzustands-Fehlermodelle übertragen.

6.1.3 Statistische Abhängigkeiten in BN-basierten Fehlermodellen

Eine wesentliche Aufgabe bei der Berechnung von BN ist die korrekte Auswertung von Zustandswahrscheinlichkeiten im Fall von statistischen Abhängigkeiten zwischen einzelnen Zuständen verschiedener Knoten. Diese entstehen, wenn Zufallsvariablen, die jeweils von Einflüssen gemeinsamer Vorgängerknoten bedingt werden, innerhalb des Netzwerks in einem Knoten miteinander in Bezug gesetzt werden.

Sind beispielsweise für eine Fehleranalyse zwei Fehler jeweils vom Vorliegen derselben Ursache abhängig, so sind deren Wahrscheinlichkeiten nicht unabhängig voneinander, sondern

bedingt unabhängig. Dieser grundlegende Effekt wird in der Literatur zu BN intensiv behandelt. So existieren diverse Theorien und Lösungsalgorithmen, die dies geeignet kompensieren (vgl. unter anderem [Lauritzen88, Pearl00, Darwiche08]). Diese Arbeiten legen den Fokus jedoch auf das gesamte Netzwerk als solches und betrachten nicht die einzelnen aussagenlogischen Beziehungen im Netzwerkmodell, die zwischen den einzelnen Zuständen der Zufallsgrößen bestehen. Stochastische Abhängigkeiten einzelner Werte der Zufallsgrößen werden somit nicht im Detail analytisch behandelt und aussagenlogisch interpretiert. Einzig in [Darwiche02, Poon11] wurde in begrenztem Umfang gezeigt, dass einzelne Zustände von Elternknoten gemäß logischer Grundoperationen miteinander verrechnet werden. Dort werden jedoch ausschließlich jeweils zwei binäre Zufallsgrößen betrachtet sowie eine auf den dort gegebenen Kontext spezifizierte Systematik für deren Auswertung, die sich von Problemstellung und Ansatz dieser Arbeit prinzipiell unterscheidet. In konkret auf die Fehlermodellierung mit BN bezogenen Arbeiten im Kontext der technischen Zuverlässigkeit wurde dies bislang ebenfalls nicht eingehender diskutiert. So existiert in Bezug auf die technische Zuverlässigkeit und die Fehlermodellierung bislang keine ausdrückliche arithmetische Darstellung und Deutung der einzelnen logischen Beziehungen, die im Rahmen von Inferenznetzwerken umgesetzt werden.

Im vorigen Abschnitt wurde bereits ein prinzipiell zu [Darwiche02] vergleichbarer, dabei jedoch umfassenderer Ansatz logischer Beziehungen Überlagerung mehrwertiger Zufallsgrößen beschrieben. Dieser ermöglicht eine analytische Darstellung und zugleich die logische Interpretation der Inferenzbeziehungen im BN im Einzelnen. So kann gezeigt werden, wie und inwieweit damit Beziehungen in Fehlermodellen auf Basis von BN in aussagenlogischen Termen darstellbar sind. Zudem werden Zusammenhänge unter gegebenen stochastischen Abhängigkeiten untersucht, was auf Grundlage zuvor dargestellten mengentheoretischen Betrachtungen mehrwertiger diskreter Zufallsgrößen möglich ist. Im Zuge dieser Untersuchungen wird die Verwendung von BN und dafür verfügbare Lösungsalgorithmen zur Implementierung komplexer Fehlermodelle verifiziert. Dies wiederum erlaubt die Erschließung deren methodischer Möglichkeiten für die Gestaltung von System-Fehlermodellen anhand von BN.

6.2 Komplexe Fehlermodelle in BN

Das Prinzip der BN wurde bereits extensiv erforscht und darf als bewiesen und bewährt gelten. Dessen Verwendung für die Fehlermodellierung ist im zuvor erläuterten Rahmen bereits Stand der Wissenschaft und Technik und demnach keine grundsätzlich offene Frage. Für deren Berechnung sind diverse Algorithmen verfügbar, die stochastische Abhängigkeiten kom-

pensieren. Die Betrachtung spezifischer Zusammenhänge einzelner logischer Beziehungen und Abhängigkeiten zwischen den Zuständen der Variablen eines BN wurde hingegen wie zuvor erläutert nicht umfassend untersucht. Ebenso besteht keine dementsprechende Grundlage zur analytischen Betrachtung deren Abhängigkeiten.

Hiervon ausgehend wird nachfolgend gezeigt, welche logischen Zusammenhänge in Inferenznetzen konkret dargestellt werden und wie sich diese arithmetisch zueinander verhalten. Dieser vorbereitende Schritt dient darauffolgend dazu, die folgenden Teilprobleme hinsichtlich der methodischen Fehleranalyse im Kontext von BN zu charakterisieren und zu verifizieren:

- komplexe Fehlermodellierung mehrwertiger Zufallsgrößen anhand von BN
- bedingte Wahrscheinlichkeiten zur Darstellung von Ungewissheit von Folgen
- probabilistische Abhängigkeiten

6.2.1 Arithmetische Grundstruktur der Inferenz in BN

Im Rahmen des in Kapitel 4 dargestellten Schemas können die elementaren Zustandskombinationen einem Zustand des Verbunds zugeordnet werden, der soweit zutreffend mit einer definierten bedingten Wahrscheinlichkeit folgen kann. Diese Wahrscheinlichkeiten werden für jeden Folgezustand kombiniert, was deren Disjunktion im aussagenlogischen Sinn entspricht. Da diese elementaren Schnittmengen schemabedingt gegenseitig exklusiv sind, entspricht deren Disjunktion grundsätzlich einem exklusiven ODER im aussagenlogischen Sinn. Die Überlagerung mehrwertiger Zufallsgrößen A, B, … ergibt dabei die Menge aller elementaren Schnittmengen $a_i b_j$ … aus den jeweils möglichen Zustandskombinationen:

$$P(a_i b_j \dots) = P(a_i) \cdot P(b_j) \cdot \dots \tag{6.01}$$

Die Gesamtheit der Wahrscheinlichkeiten aller Zustandskombinationen eines Kindknotens X der Elternknoten A und B im Netzwerk kann als Matrix $P(AB \dots | A, B, \dots)$ der Überlagerung der Zufallsgrößen A, B,… aufgefasst werden, die durch das kartesische Produkt entsteht:

$$P(AB \dots | A, B, \dots) = P(A) \otimes P(B) \dots \tag{6.02}$$

Wie in Kapitel 5 zudem beschrieben wurde, kann jeder dieser elementaren Schnitte mit einer bedingten Wahrscheinlichkeit $P(x_\xi | a_i b_j)$ einem Folgezustand x_ξ der Kindvariablen zugeordnet werden. Dies entspricht dem Faktor $\delta_{a_i b_j \dots \to x_\xi}$ der hierfür in Kapitel 5.2.4 einführt wurde. Diese bedingten Wahrscheinlichkeiten sind als Matrix $P(X | AB \dots)$ interpretierbar.

$$P(X|A,B,\dots) = P(X|AB\dots)\cdot P(AB|A,B,\dots) \tag{6.03}$$

Diese ist inhaltlich identisch zu der in [Pearl 82, Kim83] beschriebenen Matrix bedingter Wahrscheinlichkeiten $M(B|A)$ mit den Elementen $m(B|A)_{ij} = P(b_j|a_i)$ und kann daher mit dem Ausdruck $\mathrm{P(x_\xi|A,B,\dots)}$ verallgemeinert dargestellt werden. Die Matrix enthält die Einträge der CPT. Aufgrund der gegenseitigen Exklusivität der einzelnen Zustandskombinationen ($a_ib_j\dots$) addieren sich die jeweils einem einzelnen Folgezustand x_ξ zugeordneten Wahrscheinlichkeiten. Somit ergibt sich als dessen Wahrscheinlichkeit $P(x_\xi)$:

$$\begin{aligned} P(x_\xi) &= P(x_\xi|AB\dots)\cdot P(AB\dots|A,B,\dots) \\ &= \Sigma_{i,j,\dots}\{P(x_\xi|a_ib_j\dots)\cdot P(a_ib_j\dots)\} \end{aligned} \tag{6.04}$$

Sind $A,B,\dots$ in einem Netzwerkgraphen $P(X|A,B,\dots)$ voneinander unabhängig, gilt für die Wahrscheinlichkeitsverteilung der Zufallsgröße X somit:

$$P(X) = \begin{bmatrix} P(x_0) \\ P(x_1) \\ \dots \\ P(x_\xi) \\ \dots \\ P(x_k) \end{bmatrix} = \begin{bmatrix} P(x_0|AB\dots)\cdot P(AB\dots|A,B,\dots) \\ P(x_1|AB\dots)\cdot P(AB\dots|A,B,\dots) \\ \dots \\ P(x_\xi|AB\dots)\cdot P(AB\dots|A,B,\dots) \\ \dots \\ P(x_k|AB\dots)\cdot P(AB\dots|A,B,\dots) \end{bmatrix} = \begin{bmatrix} \Sigma_{i,j,\dots}[P(x_0|a_ib_j\dots)\cdot P(a_ib_j\dots)] \\ \Sigma_{i,j,\dots}[P(x_1|a_ib_j\dots)\cdot P(a_ib_j\dots)] \\ \dots \\ \Sigma_{i,j,\dots}[P(x_\xi|a_ib_j\dots)\cdot P(a_ib_j\dots)] \\ \dots \\ \Sigma_{i,j,\dots}[P(x_k|a_ib_j\dots)\cdot P(a_ib_j\dots)] \end{bmatrix} \tag{6.05}$$

Das Schema gilt für beliebig viele Variablen, die theoretisch jeweils beliebig viele diskrete Zustände aufweisen können. Durch bestimmte Kombinationen entstehende bedingte Unabhängigkeiten (s. Kapitel 5.2.3) müssen gleichwohl bei der Auswertung berücksichtigt werden, was an späterer Stelle aufgegriffen wird. Zunächst jedoch interessiert die grundlegende Form der arithmetischen Struktur des Netzwerkschemas. Dafür werden alle Größen vorerst als voneinander unabhängig angenommen.

Für die Matrix bedingter Wahrscheinlichkeiten gilt ferner die Bedingung, dass für jede Zustandskombination $P(a_ib_j\dots)$ die Summe der dieser zugeordneten bedingten Wahrscheinlichkeiten $\Sigma_\xi[P(x_\xi|A,B,\dots)] = 1$ ist. Dies ist in BN demnach jede Spalte einer CPT [Pearl 85]. Dies bedeutet, dass in der Darstellung nach obigem Beispiel für die ausschließlich binäre Betrachtung von Zuständen in jeder Spalte nur ganzzahlige Werte im Intervall [0;1] vorkommen und jeweils genau einmal die Ziffer 1 aufgeführt wird.

6.2.2 Aussagenlogische Interpretation der Beziehungen zwischen Eltern- und Kindknoten

Nach dem zuvor dargestellten arithmetischen Grundschema können logische Verknüpfungen zwischen Eltern- und Kindknoten im Stil der in Kapitel 5 erarbeiteten Grundlagen dargestellt und berechnet werden. So kann am Beispiel des ODER-Knotens in BN nach [Bobbio01] konkret gezeigt werden, auf welcher arithmetischen Grundlage dies basiert. Für zwei zweiwertige Variablen A und B gilt nach (6.05) allgemein:

$$P(X|AB) = \begin{bmatrix} P(x_0|AB) \\ P(x_1|AB) \end{bmatrix} = \begin{bmatrix} P(x_0|a_0b_0) & P(x_0|a_0b_1) & P(x_0|a_1b_0) & P(x_0|a_1b_1) \\ P(x_1|a_0b_0) & P(x_1|a_0b_1) & P(x_1|a_1b_0) & P(x_1|a_1b_1) \end{bmatrix} \tag{6.06}$$

Sei x_1 der Zustand der inklusiven Disjunktion (ODER-Operation) der Zustände a_1 und b_1 sowie x_0 dessen Komplement. Somit ist:

$$\begin{aligned} P(X|AB) &= \begin{bmatrix} P(x_0|a_0b_0) & P(x_0|a_0b_1) & P(x_0|a_1b_0) & P(x_0|a_1b_1) \\ P(x_1|a_0b_0) & P(x_1|a_0b_1) & P(x_1|a_1b_0) & P(x_1|a_1b_1) \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix} \end{aligned} \tag{6.07}$$

Die Wahrscheinlichkeitsverteilung des Kindknotens $P(X|A,B)$ ist damit:

$$P(X|A,B) = P(X|AB\ldots) \cdot P(AB|A,B,\ldots) = \begin{bmatrix} \Sigma_{i,j}\left[P\left(x_0|a_ib_j\right) \cdot P\left(a_ib_j\right)\right] \\ \Sigma_{i,j}\left[P\left(x_1|a_ib_j\right) \cdot P\left(a_ib_j\right)\right] \end{bmatrix}$$

$$= \begin{bmatrix} P(x_0|a_0b_0)P(a_0b_0) + P(x_0|a_0b_1)P(a_0b_1) + P(x_0|a_1b_0)P(a_1b_0) + P(x_0|a_1b_1)P(a_1b_1) \\ P(x_1|a_0b_0)P(a_0b_0) + P(x_1|a_0b_1)P(a_0b_1) + P(x_1|a_1b_0)P(a_1b_0) + P(x_1|a_1b_1)P(a_1b_1) \end{bmatrix}$$

$$\begin{aligned} &= \begin{bmatrix} 1 \cdot P(a_0b_0) + 0 \cdot P(a_0b_1) + 0 \cdot P(a_1b_0) + 0 \cdot P(a_1b_1) \\ 0 \cdot P(a_0b_0) + 1 \cdot P(a_0b_1) + 1 \cdot P(a_1b_0) + 1 \cdot P(a_1b_1) \end{bmatrix} \\ &= \begin{bmatrix} P(a_0)P(b_0) \\ P(a_0)P(b_1) + P(a_1)P(b_0) + P(a_1)P(b_1) \end{bmatrix} \end{aligned} \tag{6.08}$$

Berücksichtigt man die Konvention im Kontext dieser Arbeit nach Kapitel 5.1.2 (vgl. Tabelle 5.1), dass a_1 und b_1 jeweils Fehlzustände von A und B repräsentieren, sowie a_0 und b_0 die für die jeweilige Funktionsfähigkeit stehen, lässt sich dies derart interpretieren:

$$\begin{bmatrix} P(x_0) \\ P(x_1) \end{bmatrix} = \begin{bmatrix} P(a_0 \cap\ b_0) \\ P(a_1 \cup\ b_1) \end{bmatrix} = \begin{bmatrix} P('Funktion') \\ P('Fehler\ A,B\ oder\ Aund B') \end{bmatrix} \tag{6.09}$$

Grundsätzlich werden auf diese Weise alle möglichen Kombinationen von Zuständen der beteiligten Zufallsgrößen und somit jede Fehlerkombination einer Gruppe von Komponenten einem Folgezustand eindeutig zugeordnet. Analog zu der Herleitung in Kapitel 5 besteht die

Wahrscheinlichkeit jeder Zustandskombination aus dem Produkt der sich jeweils schneidenden Zustände (Konjunktion). Da diese einzelnen Zustandskombinationen gegenseitig exklusiv sind, erfolgt deren Disjunktion trivial durch Addition der Wahrscheinlichkeitswerte (s. Kapitel 4). Wie im nachfolgenden Kapitel gezeigt wird, können in diesem Schema komplexe Fehlermodelle von Systemen in analoger Weise aufgebaut werden. Diese sind aufgrund der probabilistischen Grundlage konsistent, da dies auch für BN gilt [Pearl82].

6.2.3 Probabilistisch integrale Fehlermodelle in BN

Dadurch, dass einzelne Beziehungen zwischen den Zuständen der Eltern- und Kindknoten in BN aussagenlogisch interpretiert werden können, ist es möglich, spezifische Ursache-Folge-Beziehungen zwischen einzelnen Zuständen in probabilistisch integralen Modellen umzusetzen. So kann das Beispiel aus Kapitel 5.3.3 als BN implementiert werden, in dem die Zustände des Kindknotens X von den Kombinationen der Zustände der voneinander unabhängigen Elternknoten A und B abhängig sind (s. Bild 6.1 links). Die logischen Beziehungen zwischen einzelnen Zuständen der Elternknoten entsprechen dabei den jeweiligen Gruppierungen der möglichen elementaren Zustandskombinationen der beiden Elternknoten (s. Bild 6.1 rechts).

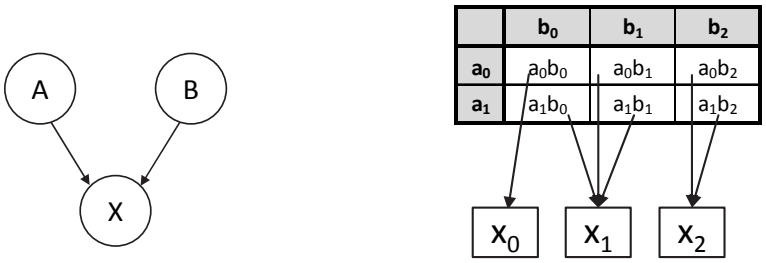


Bild 6.1: Einflussgraph (links), sowie Matrix elementarer Zustandskombinationen (rechts)

Dies entspricht folgendem Gleichungssystem:

$$P(X|A,B) = \begin{bmatrix} P(a_0 \cap b_0) \\ P(a_1 \cup b_1) \\ P\left(b_2 \underline{\cup} (a_1 \cap b_2)\right) \end{bmatrix} = \begin{bmatrix} P(a_0)P(b_0) \\ P(a_0)P(b_1) + P(a_1)P(b_0) + P(a_1)P(b_1) \\ P(a_0)P(b_2) + P(a_1)P(b_2) \end{bmatrix} \tag{6.10}$$

Beispielhaft gelten für die Variablen A und B frei gewählte Wahrscheinlichkeitswerte:

$$P(A) = \begin{bmatrix} 0{,}9 \\ 0{,}1 \end{bmatrix}, \quad P(B) = \begin{bmatrix} 0{,}99 \\ 0{,}005 \\ 0{,}005 \end{bmatrix}$$

Die Wahrscheinlichkeiten der elementaren Zustandskombinationen für $P(AB|A,B) = P(A) \otimes P(B)$ (Glg. 6.02) sind in Bild 6.2 dargestellt, worin deren Zuordnung zu den Zuständen x_ξ symbolisiert ist.

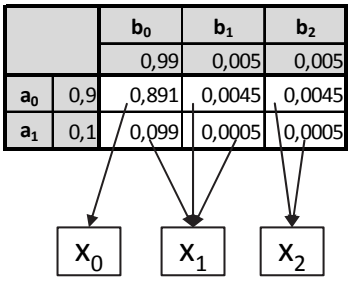


Bild 6.2: Matrix der Wahrscheinlichkeiten möglicher Zustandskombinationen für $P(AB|A,B)$

Daraus ergibt sich für X aufgrund des Gleichungssystems 6.10:

$$P(X|A,B) = \begin{bmatrix} 0{,}99 \\ 0{,}104 \\ 0{,}005 \end{bmatrix}$$

Dies kann wie in Bild 6.3 links gezeigt in Form eines BN zu implementiert werden, was die darin gezeigten Wahrscheinlichkeitswerte entsprechend ergibt (s. Bild 6.3 rechts).

X	a_0			a_1		
	a_0b_0	a_0b_1	a_0b_2	a_1b_0	a_1b_1	a_1b_2
x_0	1	0	0	0	0	0
x_1	0	1	0	1	1	0
x_2	0	0	1	0	0	1

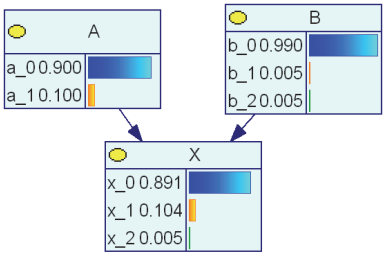


Bild 6.3: CPT der logischen Beziehungen zwischen Knoten nach Bild 6.1 (links); resultierende Wahrscheinlichkeitsverteilung des Knoten X (rechts), berechnet mit [GeNIe10]

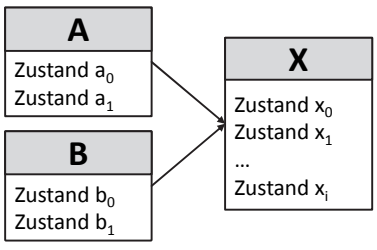
Das Verfahren gilt für beliebige Anzahlen von Variablen und deren Zustände prinzipiell in gleicher Weise. Für größere Anzahlen von Variablen und deren Zustände erhöht sich die Anzahl an kombinatorischen Möglichkeiten, was die Nachvollziehbarkeit und Zuordnung der einzelnen Werte zu den Zuständen der Kindvariablen erschwert und nur bis zu einem gewissen Umfang praktisch handhabbar erscheint. Diese Problematik bleibt in der grundlegenden Untersuchung zunächst jedoch unberücksichtigt und wird im Zuge der Ergebnisdiskussion in Kapitel 8 wieder aufgegriffen, wo Möglichkeiten zur Komplexitäts- beziehungsweise Aufwandsreduktion im Anwendungskontext aufgezeigt werden.

6.3 Modellierung von Ungewissheit in Folgebeziehungen

Wie in Kapitel 5.2.4 bereits ausgeführt wurde, können Wahrscheinlichkeiten von Zustandskombinationen anteilig mehreren Folgezuständen zugeordnet werden. Ein vergleichbarer Ansatz liegt der ETA [DIN-25419:85] (s. Kapitel 2.3.5) zugrunde, in der bedingte Wahrscheinlichkeiten zur probabilistischen Bewertung alternativ möglicher Ausgänge unter der Bedingung jeweils unterschiedlich wahrscheinlicher Randbedingungen und Ereignisverkettungen in Modellen abgebildet werden. Das dieser Methode zugrundeliegende Prinzip kann in die in den CPT anzugebenden bedingten Wahrscheinlichkeiten in BN zur Fehlermodellierung direkt implementiert werden.

Zu diesem Zweck wird in den CPT die jeweilige bedingte Wahrscheinlichkeitsverteilung für jede mögliche Kombination der Zustände der darauf weisenden Elternknoten aufgeführt. Diese Verteilung weist die Korrelation der jeweiligen Zustandskombination zu den möglichen Folgezuständen des Kindknotens auf. Die Einträge des CPT, die nach [Pearl82] in der Form „ … $wenn\ A_i$ … $dann\ X_j$ …“ interpretiert werden können, lassen daher auch eine umfassendere Deutung zu. So gilt für die Zuordnung einer spezifischen Zustandskombination der Elternknoten $A, B, \ldots$ zu einem gemeinsamen Kindknoten X:

- wenn die Zustände a_i und b_j …usw. zutreffen,
- dann sind die Zustände x_p oder x_q …usw. zutreffend,
- jeweils anteilig mit der Wahrscheinlichkeit $\delta_{b_j \to x_p}$ bzw. $\delta_{b_j \to x_q}$ … usw.



{A,B} →C	a_0		a_1	
	a_0b_0	a_0b_1	a_1b_0	a_1b_1
x_0	$\delta_{a0b0\to x0}$	$\delta_{a0b1\to x0}$	$\delta_{a1b0\to x0}$	$\delta_{a1b1\to x0}$
x_1	$\delta_{a0b0\to x1}$	$\delta_{a0b1\to x1}$	$\delta_{a1b0\to x1}$	$\delta_{a1b1\to x1}$
…	…	…	…	…
x_i	$\delta_{a0b0\to xi}$	$\delta_{a0b1\to xi}$	$\delta_{a1b0\to xi}$	$\delta_{a1b1\to xi}$

Bild 6.4: Repräsentation aussagenlogischer Beziehungen und anteilige Zuordnung zu Folgen in CPT

So kann in Bild 6.4 für jeden Folgezustand x_i aus der CPT dargestellt werden, welche Ursachen der einwirkenden Größen mit welcher Wahrscheinlichkeit jeweils alternativ zu welcher Folge führt. Das Schema ist nach [Pearl85] vollständig und konsistent.

Das wiederum hat eine für die Modellierung von Fehlerauswirkungen relevante Konsequenz. Da die exhaustive Folgevariable X aus diskreten und exklusiven Zuständen besteht, kann eine Zustandskombination $\{a_i b_j\}$ der einwirkenden Zufallsgrößen A und B jeweils nur anteilig auf

die diskreten Folgezustände aufgeteilt werden. Ein gleichzeitiges Vorliegen zweier verschiedener Folgezustände ist nicht darstellbar. Soll dies entsprechend im Modell berücksichtigt werden, muss dies als ein separater Zustand definiert werden, der das Vorliegen der simultan auftretenden Konsequenzen zusammenfassend repräsentiert. In Bild 6.5 ist solch eine kombinierte Folge beispielhaft für die Zustände x_1 und x_2 veranschaulicht. Je ein Anteil der Kombination $(a_1 b_1)$ wird darin der Folge x_1, der Folge x_2 und dem Mischzustand $x_{1,2}$ für gleichzeitiges Eintreten zugerechnet.

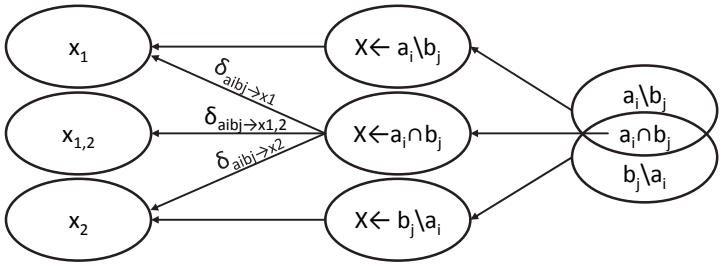


Bild 6.5: erforderliche Unterscheidung von exklusiven Zuständen in Fällen des alternativen Vorliegens (x_1, x_2) oder simultanen Vorliegens ($x_{1,2}$) von Folgesymptomatiken

6.4 Stochastische Abhängigkeiten zwischen Zuständen mehrwertiger Zufallsgrößen

Mit der im vorangegangenen Abschnitt dargestellten Systematik können individuell strukturierte probabilistische Ursache-Wirkungs-Netzwerke gebildet werden. Wenn alle Netzwerkbeziehungen ein-eindeutig und alle Beziehungen global zu einem gemeinsamen abschließenden Kindknoten konvergieren, bestehen keine weitergehenden stochastischen Abhängigkeiten über die bedingten Eltern-Kind-Abhängigkeiten hinaus. Die Gleichungen für ein solches einfaches Netzwerk mit ein-eindeutigen Zuordnungen von Eltern- zu Kindknoten können analytisch und arithmetisch so ausgewertet werden, wie es in den vorangegangenen Teilkapiteln bereits dargestellt wurde.

Bestehen an Knoten des Netzwerks jedoch mehrdeutige Einflussbeziehungen weist der gerichtete azyklische Graph jedoch Verzweigungen und Maschen auf. Diese Topologien stellen typischerweise zusätzliche Formen probabilistischer Abhängigkeiten zwischen den Knoten dar, wenn beispielsweise Einflüsse von Elternknoten in einen Kindknoten einfließen, die von gemeinsamen Vorgängern abhängig sind. Diese Abhängigkeit wird als bedingte Unabhängigkeit bezeichnet (vgl. Kapitel 5.2.3), die sich auf die resultierende Wahrscheinlichkeitsverteilung auswirkt. So kann eine Variable Einfluss auf ihre Kindvariable haben und zugleich auf ihre Nachbarvariable (s. Bild 6.6 links), die schließlich die gemeinsame Kindvariable beeinflusst. In ähnlicher Weise kann eine Ursprungsvariable zwei Kindknoten haben, die ihrerseits wiederum eine gemeinsame Kindvariable beeinflussen, wie in Bild 6.6 rechts

dargestellt ist. Solche Fälle könnten beispielsweise durch ein Bauteil gegeben sein, dessen Fehler sowohl die Funktion der eigenen Baugruppe beeinträchtigt, als auch die eines Nachbarbauteils beziehungsweise einer Nachbarbaugruppe. Diese Fälle werden nachfolgenden Abschnitt im Kontext der systemischen Fehlermodellierung diskutiert.

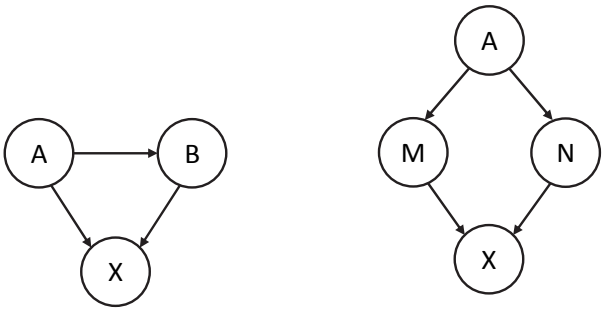


Bild 6.6: Abhängigkeit mehrerer Zufallsgrößen von einer gemeinsamen Elternvariablen

In diesem Unterabschnitt werden die arithmetischen Beziehungen zwischen einzelnen Zuständen in solchen Beziehungsschemen umfassender betrachtet. Schwerpunkt dabei ist der Nachweis deren logischen Interpretation und arithmetischen Auswertung, sowie deren Validierung als methodisches Werkzeug zur Fehlermodellierung.

6.4.1 Ansatz zur Validierung

Die arithmetischen und probabilistischen Strukturen dieser Netzwerktopologien werden aus zwei unterschiedlichen Gründen analytisch untersucht. Zum einen ist die Kenntnis der Zusammenhänge wichtig zur korrekten probabilistischen Interpretation der in BN implementierten Fehlermodelle. Zudem wird dabei das arithmetische Verfahren hinsichtlich der Betrachtung solcher probabilistischer Abhängigkeiten verifiziert. Dies geschieht im Zuge von Berechnungen auf drei Wegen:

- analytische Berechnung mittels elementarer Schnittmengen aus der vollständigen Überlagerung der mehrwertigen Zufallsgrößen
- analytische Berechnung mittels gebräuchlicher Terme für logische Operationen
- Berechnung als BN-Modell mit exaktem Lösungsalgorithmus

Der letztgenannte Weg zur Berechnung des BN anhand des Clustering-Algorithmus ist von den beiden anderen grundlegend verschieden und ermöglicht einen weiteren, unabhängigen Weg zur Verifikation. Der Algorithmus beruht auf einem graphentheoretischen Verfahren [Lauritzen88, Darwiche08], das Abhängigkeiten im Netzwerk anhand geeigneter Zusammenfassungen von Knoten zu Gruppen eliminiert. Er beruht daher im Unterschied zu den anderen beiden analytischen Rechenwegen nicht auf mengentheoretischer Analyse und

Elimination von Abhängigkeiten einzelner Werte der Zufallsgrößen auf Basis von Axiomen. Aufgrund dieser Diversität ist anzunehmen, dass das Potenzial gleichartiger Irrtümer oder grundlegender Berechnungsfehler durch die Verschiedenheit der Auswerteverfahren minimiert wird oder ausgeschlossen ist. Dies reduziert die Wahrscheinlichkeit gleichlautend falscher Ergebnisse und eignet sich dadurch zum Nachweis der Korrektheit der Ergebnisse und der Rechenverfahren. Diese drei Ansätze dienen der wechselseitigen Validierung der in Kapitel 5 erarbeiteten theoretischen Grundlage und deren Anwendung als BN-Fehlermodelle.

6.4.2 Einfluss zwischen Elternknoten

Im Hinblick auf die Anwendung solcher Fehlermodelle im Kontext der Fehleranalyse technischer Systeme sei beispielhaft angenommen, ein Fehlzustand eines Bauteils $\boldsymbol{A}$ übe eine einen Ausfall begünstigende Wirkung auf ein anderes Bauteil $\boldsymbol{B}$ aus. So kann der Fehlzustand des Bauteils $\boldsymbol{A}$ die Wahrscheinlichkeit eines Defekts des Nachbarbauteils $\boldsymbol{B}$ erhöhen. Dies ist beispielsweise der Fall, wenn eine fehlerbedingt hohe Eigenerwärmung des Bauteils $\boldsymbol{A}$ einen nicht spezifikationsgemäßen Wärmeeintrag in Bauteil $\boldsymbol{B}$ bewirkt (s. Kapitel 4.3.2, Sekundärdefekt). Die Wahrscheinlichkeitsverteilung der Zufallsgröße $\boldsymbol{B}$ in diesem Modell ist abhängig von $\boldsymbol{A}$. Dies wird in diesem BN-Fehlermodell durch einen Pfeil von Komponente $\boldsymbol{A}$ zu Komponente $\boldsymbol{B}$ symbolisiert. Sind $\boldsymbol{A}$ und $\boldsymbol{B}$ Unterkomponenten von Komponentenverbund $\boldsymbol{X}$ (vgl. Bild 6.6 links), muss die statistische Abhängigkeit der Komponente $\boldsymbol{B}$ von $\boldsymbol{A}$ bei der Berechnung der Wahrscheinlichkeitsverteilung des Komponentenverbunds $\boldsymbol{X}$ berücksichtigt werden. Hinter dem Symbol des Pfeils von $\boldsymbol{A}$ zu $\boldsymbol{B}$ jedoch verbergen sich mehrere konkrete Einflussbeziehungen zwischen den jeweiligen Zuständen.

Im Netzwerk, beispielsweise, links in Bild 6.6, das aus den Zufallsvariablen $\boldsymbol{A}$, $\boldsymbol{B(B|A)}$ und $\boldsymbol{X(X|A,B)}$ besteht ist $\boldsymbol{X}$ abhängig von $\boldsymbol{A}$ und $\boldsymbol{B}$, wobei $\boldsymbol{B}$ selbst vom Zustand der Komponente $\boldsymbol{A}$ abhängt. Nach Gleichung (5.34) gilt für die Zustände $\boldsymbol{b_j}$:

$$b_j = \underline{\cup}_i \left[\delta_{a_i \to b_j} \cdot a_i\right] \tag{6.11}$$

$$P(b_j) = \Sigma_i\left[P(b_j|a_i)\, P(a_i)\right] \tag{6.12}$$

Die Terme in logischer Algebra für $\boldsymbol{b_i}$ sind:

$$b_0 = (\delta_{a_0 \to b_0} a_0) \,\underline{\cup}\, (\delta_{a_1 \to b_0} a_1) \tag{6.13}$$

$$b_1 = (\delta_{a_0 \to b_1} a_0) \,\underline{\cup}\, (\delta_{a_1 \to b_1} a_1) \tag{6.14}$$

Für x_i gilt:

$$x_0 = a_0 \cap b_0 = a_0 \cap \left[\left(\delta_{a_0 \to b_0} a_0\right) \underline{\cup} \left(\delta_{a_1 \to b_0} a_1\right)\right] \tag{6.16}$$

$$\begin{aligned} x_1 &= (a_0 \cap b_1) \underline{\cup} \left[(a_1 \cap b_0) \underline{\cup} (a_1 \cap b_1)\right] \\ &= a_0 \cap \left[\left(\delta_{a_0 \to b_1} a_0\right) \underline{\cup} \left(\delta_{a_1 \to b_1} a_1\right)\right] \underline{\cup} a_1 \cap \left[\left(\delta_{a_0 \to b_0} a_0\right) \underline{\cup} \left(\delta_{a_1 \to b_0} a_1\right)\right] \underline{\cup} a_1 \\ &\qquad \cap \left[\left(\delta_{a_0 \to b_1} a_0 \underline{\cup} \delta_{a_1 \to b_1} a_1\right)\right] \end{aligned} \tag{6.17}$$

Die logische Aussage in dem Term für x_1 entspricht dabei einer inklusiven ODER-Operation. In dem Verfahren auf Basis elementarer Schnittmengen der Zustandsüberlagerungen sind diese prinzipiell zueinander exklusiv (s. Kapitel 5) und können arithmetisch addiert werden. Die aus den exklusiv-ODER-Operationen hervorgehenden Wahrscheinlichkeiten können daher direkt ohne andernfalls erforderliche Korrekturterme aufgrund gemeinsamer Schnittmengen berechnet werden. Für die Wahrscheinlichkeitsverteilung $P(X)$ ergibt sich:

$$P(x_0) = P(a_0) \cdot P(b_0) \tag{6.18}$$

$$P(x_1) = P(a_0) \cdot P(b_1) + P(a_1) \cdot P(b_0) + P(a_1) \cdot P(b_1) \tag{6.19}$$

mit $P(B)$:

$$P(b_0) = P(b_0|a_0) \cdot P(a_0) + P(b_0|a_1) \cdot P(a_1) \tag{6.20}$$

$$P(b_1) = P(b_1|a_0) \cdot P(a_0) + P(b_1|a_1) \cdot P(a_1) \tag{6.21}$$

Gilt:

$$P(x_0) = P(a_0) \cdot [P(b_0|a_0) \cdot P(a_0) + P(b_0|a_1) \cdot P(a_1)] \tag{6.22}$$

$$\begin{aligned} P(x_1) = \; & P(a_0) \cdot [P(b_1|a_0) \cdot P(a_0) + P(b_1|a_1) \cdot P(a_1)] + P(a_1) \\ & \cdot [P(b_0|a_0) \cdot P(a_0) + P(b_0|a_1) \cdot P(a_1)] + P(a_1) \\ & \cdot [P(b_1|a_0) \cdot P(a_0) + P(b_1|a_1) \cdot P(a_1)] \end{aligned} \tag{6.23}$$

Mit den Axiomen nach [Peano1888] gilt $P(a_i) \cdot P(a_i) = P(a_i)$ und $P(a_0) \cdot P(a_1) = 0$, weshalb

$$P(x_0) = P(a_0) \cdot P(b_0|a_0) \tag{6.24}$$

$$P(x_1) = P(a_0) \cdot P(b_1|a_0) + P(a_1) \cdot P(b_0|a_1) + P(a_1) \cdot P(b_1|a_1) \tag{6.25}$$

ist. Gelten als Beispiel die zufällig gewählten Zahlenwerte

$$A = \begin{bmatrix} a_0 \\ a_1 \end{bmatrix} = \begin{bmatrix} 0{,}9 \\ 0{,}1 \end{bmatrix} \quad , \qquad B(B|A) = \begin{bmatrix} 0{,}9 & 0{,}5 \\ 0{,}1 & 0{,}5 \end{bmatrix}$$

so ergibt sich als Wahrscheinlichkeit für die Zustände des Verbunds X:

$$P(x_0) = 0{,}9 \cdot 0{,}9 = 0{,}81$$

$$P(x_1) = 0{,}9 \cdot 0{,}1 + 0{,}1 \cdot 0{,}5 + 0{,}1 \cdot 0{,}5 = 0{,}19$$

Eine äquivalente Berechnung ist auch nach dem Prinzip eines Fehlerbaums möglich, in dem man die bedingten Wahrscheinlichkeiten $b_1(b_1|\mathrm{a}_0)$ und $b_1(b_1|\mathrm{a}_1)$ des Fehlzustands b_1 jeweils als sich gegenseitig ausschließende Basisereignisse (exklusiv-ODER) einbindet. So gilt:

$$\begin{aligned} P(x_0) = P(a_0)P(b_0) &= P(a_0)\,[P(b_0|a_0)P(a_0) + P(b_0|a_1)P(a_1)] \\ &= P(b_0|a_0)P(a_0)P(a_0) + P(b_0|a_1)P(a_1)P(a_0) \end{aligned} \tag{6.26}$$

Reduziert mithilfe der Peano-Axiome ergibt sich daraus:

$$P(x_0) = P(b_0|a_0)P(a_0) = 0{,}9 \cdot 0{,}9 = 0{,}81$$

Analog gilt für x_1:

$$\begin{aligned} P(x_1) &= P(a_1) + P(b_1) - P(a_1)P(b_1) \\ &= P(a_1) + \big(1 - P(a_1)\big)P(b_1) = P(a_1) + P(a_0)P(b_1) \end{aligned} \tag{6.27}$$

Darin ist b_1:

$$\begin{aligned} P(b_1) &= P(b_1|a_0)P(a_0) + P(b_1|a_1)P(a_1) - 2 \cdot P(b_1|a_0)P(a_0) \cdot P(b_1|a_1)P(a_1) \\ &= P(b_1|a_0)P(a_0) + P(b_1|a_1)P(a_1) \end{aligned} \tag{6.28}$$

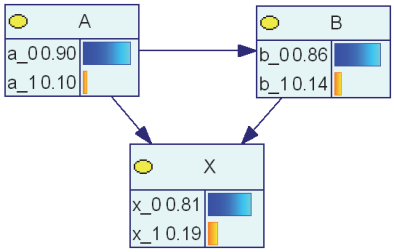
Dadurch ergibt sich

$$\begin{aligned} P(x_1) &= P(a_1) + P(a_0) \cdot [P(b_1|a_0)P(a_0) + P(b_1|a_1)P(a_1)] \\ &= P(a_1) + P(a_0)P(a_0)P(b_1|a_0) + P(a_0)P(a_1)P(b_1|a_1) \\ &= P(a_1) + P(a_0)P(b_1|a_0) \end{aligned} \tag{6.29}$$

Damit kann die Wahrscheinlichkeit des Zustands x_1 berechnet werden:

$$P(x_1) = 0{,}1 + 0{,}9 \cdot 0{,}1 = 0{,}19$$

In Bild 6.7 ist ein BN beruhend auf den Daten des Beispiels abgebildet. Die Berechnung erfolgte hier auf Basis des exakten Clustering-Verfahrens, das die statistische Abhängigkeit darin berücksichtigt. Dabei entsprechen die Ergebnisse der analytischen Rechnung auf Grundlage des Aussagenkalküls nach den Gleichungen (6.26) bis (6.29). Die Berechnung auf Basis elementarer Schnitte aller Zustandskombinationen und der bedingten Disjunktion in $B(B|A)$ aus den Gleichungen (6.11) bis (6.25) folgt das gleiche Ergebnis.



X	a_0		a_1	
	a_0b_0	a_0b_1	a_1b_0	a_1b_1
x_0	1	0	0	0
x_1	0	1	1	1

Bild 6.7: BN-Modell des Beispiels als in [GeNIe10] (links) und CPT für Variable X (rechts)

6.4.3 Einfluss gemeinsamer Ahnenknoten

In prinzipiell vergleichbarer Weise, wie die zuvor untersuchte unmittelbare Beeinflussung von Komponenten durch andere Komponenten, können in einem probabilistischen Einflussnetzwerk statistische Abhängigkeiten auch über mehrere Hierarchieebenen hinweg bedingt unabhängig bestehen (s. Bild 6.6, rechts). Ein veranschaulichendes Beispiel hierfür ist eine einzelne Fehlerursache a_1 einer Komponente A, die in zwei verschiedenen Subsystemen M und N jeweils fehlerbedingte Funktionsabweichungen m_1 beziehungsweise n_1 nach sich ziehen kann. Diese Funktionsabweichungen treten jeweils nicht in jedem Fall ein. So bewirkt a_1 die Folgen m_1 oder m_0 sowie unabhängig davon n_1 oder n_0. Die Zustände m_1 und n_1 führen im Gesamtsystem X wiederum zur gleichen Folge x_1. Liegen m_1 und n_1 jedoch zugleich vor, folgt eine andere Fehlerkonsequenz x_2. Die jeweiligen Zustände a_0, m_0, n_0 und x_0 repräsentieren die jeweiligen Zustände der Fehlerfreiheit. Falls weder m_1 noch n_1 vorliegen, herrscht x_0 im System vor. Dieses Beziehungssystem ist als Mengendiagramm (Bild 6.8, links) sowie als Projektionsschema der Einflussbeziehungen im Netzwerk (Bild 6.8, rechts) darstellbar.

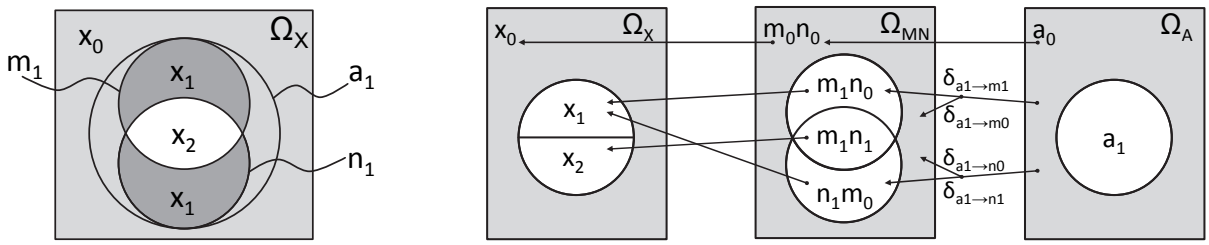


Bild 6.8: Mengendiagramme der Schnittmengen (links) und Projektionsschema der Einflussbeziehungen (rechts)

Für dieses aussagenlogische Beziehungssystem gilt:

$$m_0 = a_0 \underline{\cup} \delta_{a_1 \to m_0} a_1 \quad , \quad m_1 = \delta_{a_1 \to m_1} a_1 \tag{6.28}$$

$$n_0 = a_0 \underline{\cup} \delta_{a_1 \to n_0} a_1 \quad , \quad n_1 = \delta_{a_1 \to n_1} a_1 \tag{6.29}$$

Daher ist:

$$x_0 = m_0 \cap n_0 = \left(a_0 \underline{\cup} \delta_{a_1 \to m_0} a_1\right) \cap \left(a_0 \underline{\cup} \delta_{a_1 \to n_0} a_1\right) \tag{6.30}$$

$$\begin{aligned} x_1 &= (m_0 \cap n_1) \underline{\cup} (m_1 \cap n_0) \\ &= \left(a_0 \underline{\cup} \delta_{a_1 \to m_0} a_1\right) \cap \left(\delta_{a_1 \to n_0} a_1\right) \underline{\cup} \left(\delta_{a_1 \to m_1} a_1\right) \cap \left(a_0 \underline{\cup} \delta_{a_1 \to n_0} a_1\right) \end{aligned} \tag{6.31}$$

$$x_2 = m_1 \cap n_1 = \left(\delta_{a_1 \to m_1} a_1\right) \cap \left(\delta_{a_1 \to n_1} a_1\right) \tag{6.32}$$

Zur probabilistischen Auswertung der Gleichungen können die Teilterme arithmetisch addiert werden, da die durch sie ausgedrückten elementaren Schnittmengen gegenseitig exklusiv sind und keine Korrektur eines Anteils einer gemeinsamen Schnittmenge erforderlich ist. Aufgrund der gegenseitigen Exklusivität der Zustände a_i, a_j der Zufallsgröße A ist $(a_1 \cap a_0) = \{\}$, beziehungsweise $P(a_1 \cap a_0) = 0$. Daher gilt: $a_i \cdot a_j = 0$ für $i \neq j$ und $\{ai, aj\} \in A$ und es gilt:

$$\begin{aligned} P(x_0) &= P(a_0)P(a_0) + P(n_0|a_1)P(a_0)P(a_1) + P(m_0|a_1)P(a_1)P(n_0|a_1)P(a_1) \\ &= P(a_0) + P(m_0|a_1)P(n_0|a_1)P(a_1) \end{aligned} \tag{6.33}$$

$$\begin{aligned} P(x_1) = {} & P(n_0|a_1)P(a_0)P(a_1) + P(m_0|a_1)P(a_1)P(n_0|a_1)P(a_1) + P(m_1|a_1)P(a_1)P(a_0) \\ & + P(m_1|a_1)P(a_1)P(n_0|a_1)P(a_1) \\ = {} & P(m_0|a_1)P(a_1)P(n_0|a_1)P(a_1) + P(m_1|a_1)P(n_0|a_1)P(a_1) \end{aligned} \tag{6.34}$$

$$P(x_2) = P(m_1|a_1)P(a_1)P(n_1|a_1)P(a_1) = P(m_1|a_1)P(n_1|a_1)P(a_1) \tag{6.35}$$

Mit zufällig gewählten beispielhaften Werten der Knoten A, M und N

$$P(A) = \begin{bmatrix} P(a_0) \\ P(a_1) \end{bmatrix} = \begin{bmatrix} 0{,}5 \\ 0{,}5 \end{bmatrix}$$

$$P(M|A) = \begin{bmatrix} P(m_0|a_0) & P(m_0|a_1) \\ P(m_1|a_0) & P(m_1|a_1) \end{bmatrix} = \begin{bmatrix} 1 & 0{,}5 \\ 0 & 0{,}5 \end{bmatrix}$$

$$P(N|A) = \begin{bmatrix} P(n_0|a_0) & P(n_0|a_1) \\ P(n_1|a_0) & P(n_1|a_1) \end{bmatrix} = \begin{bmatrix} 1 & 0{,}5 \\ 0 & 0{,}5 \end{bmatrix}$$

gilt für X:

$$P(X|M,N) = \begin{bmatrix} P(x_0|m_0n_0) & P(x_0|m_0n_1) & P(x_0|m_1n_0) & P(x_0|m_1n_1) \\ P(x_1|m_0n_0) & P(x_1|m_0n_1) & P(x_1|m_1n_0) & P(x_1|m_1n_1) \\ P(x_2|m_0n_0) & P(x_2|m_0n_1) & P(x_2|m_1n_0) & P(x_2|m_1n_1) \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{6.36}$$

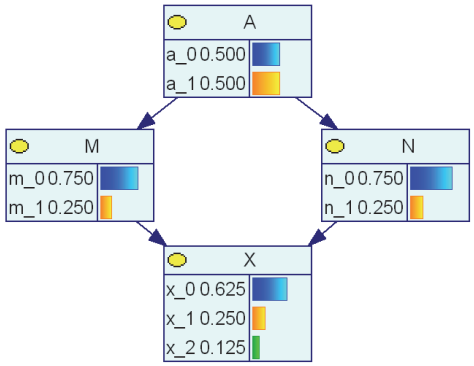
Anhand der Zahlenwerte ergibt sich daraus:

$$P(x_0) = 0{,}5 + 0{,}5 \cdot 0{,}5 \cdot 0{,}5 = 0{,}625$$

$$P(x_1) = 0{,}5 \cdot 0{,}5 \cdot 0{,}5 + 0{,}5 \cdot 0{,}5 \cdot 0{,}5 = 0{,}25$$

$$P(x_2) = 0{,}5 \cdot 0{,}5 \cdot 0{,}5 = 0{,}125$$

Dies gleicht den Ergebnissen einer analogen Berechnung in einem BN aus den Knoten M, N und X mit dementsprechendem Aufbau (Bild 6.9 links) und Wahrscheinlichkeitsverteilungen (Bild 6.9 rechts).



M	a_0	a_1
x_0	1	0,5
x_1	0	0,5

N	a_0	a_1
x_0	1	0
x_1	0	1

X	m_0		m_1	
	m_0n_0	m_0n_1	m_1n_0	m_1n_1
x_0	1	0	0	0
x_1	0	1	1	0
x_2	0	0	0	1

Bild 6.9: BN-Modell des Beispiels in [GeNIe10] (links) und CPT-Einträge der Knoten (rechts)

Überprüft man die darin implementierten Aussagen auf Grundlage der gebräuchlichen Terme für logische Operationen (s. Glgn. 2.06, 2.07, 2.08. und 2.09), so ergeben sich jeweils:

$$x_0 = m_0 \cap n_0 = \left[a_0 \cup \left(\delta_{a_1 \to m_0} a_1\right)\right] \cap \left[a_0 \cup \left(\delta_{a_1 \to n_0} a_1\right)\right] \tag{6.37}$$

$$\begin{aligned} P(x_0) &= P(m_0)P(n_0) \\ &= [P(a_0) + P(m_0|a_1)P(a_1) - 2 \cdot P(a_0)P(m_0|a_1)P(a_1)] \\ &\quad \cdot [P(a_0) + P(n_0|a_1)P(a_1) - 2 \cdot P(a_0)P(n_0|a_1)P(a_1)] \\ &= [P(a_0) + P(m_0|a_1)P(a_1)] \cdot [P(a_0) + P(n_0|a_1)P(a_1)] \\ &= P(a_0)P(a_0) + P(m_0|a_1)P(a_0)P(a_1) + P(n_0|a_1)P(a_0)P(a_1) \\ &\quad + P(m_0|a_1)P(n_0|a_1)P(a_1) \\ &= P(a_0) + P(m_0|a_1)P(n_0|a_1)P(a_1) \end{aligned} \tag{6.38}$$

$$P(x_0) = 0{,}625$$

Daraus folgen die Terme für x_1 und $P(x_1)$:

$$x_1 = m_1 \underline{\cup} n_1 = (\delta_{a_1 \to m_1} a_1) \underline{\cup} (\delta_{a_1 \to n_1} a_1) \tag{6.39}$$

$$\begin{aligned} P(x_1) &= P(m_1) + P(n_1) + 2 \cdot P(m_1)P(n_1) \\ &= P(m_1|a_1)P(a_1) + P(n_1|a_1)P(a_1) - 2 \\ &\qquad \cdot P(m_1|a_1)P(a_1)P(n_1|a_1)P(a_1) \\ &= [P(m_1|a_1) + P(n_1|a_1) - 2 \cdot P(m_1|a_1)P(n_1|a_1)]P(a_1) \\ P(x_1) &= [0{,}5 + 0{,}5 - 2 \cdot 0{,}5 \cdot 0{,}5] \cdot 0{,}5 = 0{,}25 \end{aligned} \tag{6.40}$$

sowie für x_2 und $P(x_2)$:

$$x_2 = m_1 \cap n_1 = \left(\delta_{a_1 \to m_1} a_1\right) \cap \left(\delta_{a_1 \to n_1} a_1\right) \tag{6.41}$$

$$\begin{aligned} P(x_2) &= P(m_1|a_1)P(a_1)\, P(n_1|a_1)P(a_1) \\ &= P(m_1|a_1)\, P(n_1|a_1)P(a_1) \\ P(x_2) &= 0{,}5 \cdot 0{,}5 \cdot 0{,}5 = 0{,}125 \end{aligned} \tag{6.42}$$

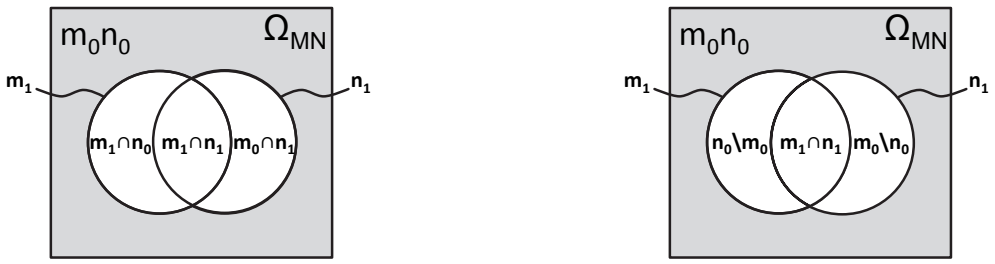


Bild 6.10: alternative Bezeichnungen der elementaren Schnittmengen in Ω_{MN}

x_1 kann alternativ auch auf Basis von m_0 und n_0 berechnet werden. Dies liefert im gegebenen Fall dasselbe Ergebnis, da die Ausdrücke $x_1 = m_1 \cup n_1$ und $x_1 = m_0 \underline{\cup} n_0$ jeweils dieselben Teilmengen bezeichnen (vgl. Bild 6.10 rechts). Setzt man zur analytischen Berechnung die Terme entsprechend an, so ist:

$$x_1 = m_0 \underline{\cup} n_0 = \left[a_0 \underline{\cup} (\delta_{a_1 \to m_0} a_1)\right] \underline{\cup} \left[a_0 \underline{\cup} (\delta_{a_1 \to n_1} a_1)\right] \tag{6.43}$$

$$
\begin{aligned}
P(x_1) = \; & P(m_1) + P(n_1) - 2 \cdot P(m_0)P(n_0) \\
= \; & [P(a_0) + P(m_0|a_1)P(a_1)] + [P(a_0) + P(n_0|a_1)P(a_1)] - 2 \\
& \cdot \left[\left(P(a_0) + P(m_0|a_1)P(a_1)\right)\left(P(a_0) + P(n_0|a_1)P(a_1)\right)\right] \\
= \; & 2 \cdot P(a_0) + P(m_0|a_1)P(a_1) + P(n_0|a_1)P(a_1) - 2 \\
& \cdot [\, P(a_0)P(a_0) + P(m_0|a_1)P(a_0)P(a_1) + P(n_0|a_1)P(a_0)P(a_1) \\
& + P(m_0|a_1)P(n_0|a_1)P(a_1)P(a_1) \,] \\
= \; & \left[\left(P(m_0|a_1) + P(n_0|a_1)\right) - 2 \cdot P(m_0|a_1)P(n_0|a_1)\right] P(a_1) \\
P(x_1) = \; & [0{,}5 + 0{,}5 - 2 \cdot 0{,}5 \cdot 0{,}5] \cdot 0{,}5 = 0{,}25
\end{aligned}
\tag{6.44}
$$

Dies stimmt ebenfalls mit allen zuvor gezeigten Berechnungen überein. Zudem zeigt die Überprüfung entsprechend gleiche Ergebnisse auch für beliebige Wahrscheinlichkeitsverteilungen der Variablen $\boldsymbol{A}$ sowie für beliebige bedingte Wahrscheinlichkeiten der Größen $\boldsymbol{M}$, $\boldsymbol{N}$ und $\boldsymbol{X}$. Dies zeigt, dass sowohl die Gleichungen anhand der elementaren Schnittmengen, als auch die Gleichungen nach den gebräuchlichen Termen für logische Operationen (s. Glgn. 2.06, 2.07, 2.08. und 2.09), wie auch die Berechnung in Form eines BN identische Ergebnisse liefern. Die verschiedenen Berechnungswege beziehungsweise Berechnungsverfahren bestätigen ihre Gültigkeit wechselseitig.

Anhand der in Kapitel 5 erörterten Grundlagen lässt sich nachvollziehen, dass das Schema auf Basis elementarer Schnittmengen (Minterme) anhand exhaustiver Zufallsgrößen auch in komplexen Zusammenhängen unverändert gilt. Die in komplexeren Modellen entstehenden Terme bauen sich aus entsprechenden Summanden auf. Deren Multiplikanden stellen Teilmengen dar, die in identischer Weise zu behandeln sind. Stochastische Abhängigkeiten sind dabei mittels der Axiome von Peano zu kompensieren, wie dies beispielsweise für Fehlerbäume in [DeLong70, Vesely81] unter anderem als Boolesche Reduktion für die klassische FTA erläutert wird.

Mit zunehmender Anzahl enthaltener Zufallsvariablen und deren Zustandsmöglichkeiten ist die analytische Berechnung jedoch zunehmend umfangreich und komplex. Mit klassischen Termen (s. Kapitel 2) für logische Operatoren kann dabei die Grenze der Praktikabilität und Nachvollziehbarkeit überschritten werden, da insbesondere für mehrere sich überlagernde Größen die Komplexität der Teilterme für Disjunktionen (ODER, XODER) in progressivem Maße zunimmt. Die Berechnung mit dem Schema elementarer Schnittmengen beinhaltet zwar im Gegensatz dazu keine im selben Maß zunehmende strukturelle Komplexität der Teilterme. Hierbei ergeben sich im Vergleich dazu einfacher nachzuvollziehende Teilterme mit

sich regelmäßig wiederholenden und vergleichsweise gut nachvollziehbaren Reduktionsschemata. Dennoch nimmt die Anzahl der Minterme mit zunehmender Zahl an Zufallsgrößen exponentiell zu, da alle Zustandskombinationen zu definieren sind. Dies stellt eine maßgebliche Restriktion für die praktische Umsetzung dar. Daher werden Berechnungen im Folgenden nicht mehr analytisch ausgeführt, sondern in Form von BN, die mit dem Clustering-Algorithmus in der Anwendungssoftware [GeNIe10] berechnet.

6.5 Zusammenfassung und Zwischenfazit

In Kapitel 5 wurde hergeleitet, wie allgemeine probabilistische Grundlagen zur Betrachtung logischer Beziehungen zwischen gegebenenfalls untereinander abhängigen mehrwertigen Zufallsgrößen zur Darstellung und Auswertung zusammenhängender, aussagenlogischer Beziehungen angewendet werden können. Ausgehend von diesen zuvor gewonnenen Erkenntnissen konnte in Kapitel 6 gezeigt werden, dass diese entsprechend auch dem Schema von BN zugrunde liegen, was in bisherigen Ansätzen nicht entsprechend berücksichtigt wurde. Im Einzelnen wurde so nachvollzogen, in welcher konkreten Weise dieses probabilistische Verfahren die Abbildung und Berechnung spezifischer logischer Beziehungen zwischen Zuständen sich beeinflussender mehrwertiger Zufallsgrößen ermöglicht. Ferner wurden aussagenlogische Zusammenhänge auch im Fall von probabilistischen Abhängigkeiten in Bezug auf jeweils einzelne spezifische Zustände der Zufallsgrößen identifiziert und deren arithmetisch korrekte Behandlung analytisch nachvollzogen.

Aufgrund der Exaktheit der Berechnungen anhand des Clustering-Algorithmus sowie des zugrundeliegenden graphentheoretischen Ansatzes, der diversitär zu den gezeigten analytischen Berechnungen ist, konnten diese gegenüber den analytischen Berechnungen verifiziert werden. Im Umkehrschluss wird daher gefolgert, dass die Umsetzung der logischen Beziehungen in BN und deren Berechnung übereinstimmend mit den analytischen Betrachtungen ist.

Ferner konnte validiert werden, dass stochastische Abhängigkeiten dabei in korrekter und nachvollziehbarer Weise kompensiert werden, wie dies wiederum der Auffassung logischer Kausalbeziehungen in technischen Fehlermodellen entspricht. Diese Erkenntnisse der vorangegangenen Abschnitte werden nachfolgend genutzt, um damit eine integrale Methodik zur Modellierung von Fehlzuständen und deren Auswirkungen im Kontext eines technischen Systems darzustellen, die sich probabilistisch entsprechend auswerten lässt.

7 Methodisches Konzept zur Fehleranalyse technischer Systeme

In den vorangegangenen Kapiteln wurde die Verwendung mehrwertiger Zufallsgrößen in Mehrzustands-Fehlermodellen in der Form probabilistischer Einflussnetzwerke grundsätzlich untersucht und verifiziert. Nachfolgend wird ein methodischer Ansatz für strukturhierarchisch orientierte Mehrzustands-Fehlermodelle ausgearbeitet, der auf diesen Grundlagen beruht. Zusammen mit dem in Kapitel vier vorbereiteten Rahmenkonzept wurde in dieser Arbeit somit bereits eine Reihe von Randannahmen für einen solchen Modellansatz festgehalten. Diese lassen sich in knapper Form folgendermaßen auflisten:

- Systeme können in mehreren hierarchischen Stufen bis hin zu einzelnen Bauteilen untergliedert werden.
- Ein angemessenes Systemverhalten ergibt sich aus der Gesamtheit der Eigenschaften und Funktionen der Unterkomponenten in Form von Bauteilverbünden und Bauteilen sowie durch deren spezifiziertes Zusammenspiel.
- Liegt eine Abweichung gegenüber explizit und implizit gegebenen Eigenschaften oder Verhaltensweisen einer Komponente vor, so stellt dies einen von gegebenenfalls mehreren möglichen Fehlzuständen dar.
- Im Fall eines Fehlzustands einer Komponente ist die uneingeschränkte Funktionsfähigkeit der dieser übergeordneten Bauteilverbünde nicht mehr gegeben und diese befinden sich selbst in einem Fehlzustand.
- Alle möglichen Fehlzustände einer Komponente sowie deren Zustand der Funktionsfähigkeit werden als diskrete und exklusive Zustände repräsentiert.
- Fehlzuständen lässt sich eine Wahrscheinlichkeit für deren Vorliegen zuordnen.
- Die Gesamtheit aller möglichen Fehlzustände einer Komponente ist zu dem Zustand der Funktionsfähigkeit komplementär und entspricht der totalen Wahrscheinlichkeit.
- Wahrscheinlichkeiten resultierender Fehlzustände, die durch verschiedene technologische Ursachen bedingt sind, können nach aussagenlogisch-probabilistischen Grundsätzen anhand der Wahrscheinlichkeiten von Ursachen und den gegebenen Verhältnismäßigkeiten der zugehörigen Fehlerbeziehungen ermittelt werden
- Beziehungen zwischen Fehlerursachen von Komponenten und resultierenden Folgezuständen betroffener Komponentenverbünde beruhen auf kausalen Beziehungen, die auf aussagenlogischer Grundlage im Sinne von Ursache-Folge-Beziehungen („Wenn…, dann…“) aufgefasst werden können.
- Ungewissheit in probabilistischem Sinne kann in Form von fallweise alternativ möglichen Folgen („Wenn…, dann… oder…“) anteilig dargestellt werden.

7.1 Differenzierung gegenüber dem Stand der Wissenschaft und Technik

In den vorangegangenen Kapiteln wurden bereits im Stand von Wissenschaft und Technik vorhandene Ansätze zur Fehlermodellierung erwähnt und in verschiedener Hinsicht charakterisiert. In diesem Abschnitt wird ein Ansatz auf Basis der zuvor erarbeiteten probabilistischen Modellgrundlage innerhalb des strukturhierarchisch gegliederten Rahmenkonzepts (s. Kapitel 4) gegenüber den bisherigen abgegrenzt.

7.1.1 Strukturierung des Fehlermodells

Zur methodischen Fehlermodellierung mit BN werden Ansätze nach [Portinale99, Weber06, Kempf08, Andrews09, Khakzad11] nicht anhand der hierarchischen Gliederung der Systemstruktur aufgebaut. In keinem der Ansätze erfolgt die Repräsentation von Komponenten gemäß der hierarchischen Gliederung des Systems als jeweils eine integrale Mehrzustands-Zufallsvariable, die alle Zustände einer Komponente darstellt. Stattdessen werden die Fehlermodelle vorrangig anhand der jeweils darzustellenden logischen Beziehung beziehungsweise des übergeordneten Analyseziels aufgebaut. Dabei werden zum einen dadurch nur Ursache-Folge-Beziehungen im Modell aufgeführt, die im Sinne der spezifischen Fragestellung relevant sind. Solche, die sich außerhalb des Analyseziels befinden, werden dagegen nicht berücksichtigt. Zum anderen entstehen dabei komplexe Netzwerke, da alle relevanten Beziehungen als explizite Einzelknoten des Netzwerkgraphen repräsentiert werden. Für komplexe Systeme beeinträchtigt dies die Nachvollziehbarkeit, da alle Ursache-Folge-Beziehungen und deren logischen Verknüpfungen als Graphenelemente abgebildet werden, was zu sehr umfangreichen Netzwerken führt [Lampis10].

In [Bobbio01, Kim11, Kim14, Portinale15] werden zwar Fehlermodelle entsprechend der hierarchischen Systemstruktur aufgebaut und die Fehlerursachen und –folgen an diesen ausgerichtet. Dabei werden auch Mehrzustands-Zufallsgrößen vereinzelt grundsätzlich erwähnt. Die konkrete Interpretation und Umsetzung der darin zu gestaltenden multiplen logischen Beziehungen erfolgte dort jedoch nicht. Dabei typischerweise im Modell abzubildende komplexe Abhängigkeiten wurden nicht als Fragestellung behandelt.

Mit dem zuvor gezeigten integralen Modellprinzip wird in dieser Arbeit ein dazu alternativer Weg verfolgt. Der strukturhierarchisch gegliederte Netzwerkgraph stellt nur Komponenten und deren Gruppierungen innerhalb des Systems explizit dar. Die logischen Beziehungen werden für jeden Knoten nicht maßgeblich durch die Graphenstruktur, sondern als Gleichungssysteme logischer Verknüpfungen von Zustandskombinationen unmittelbar in den CPT modelliert. Da Anzahl und Komplexität der Beziehungen zwischen Fehlermöglichkeiten

und Fehlerfolgen systembedingt gegeben und mitunter hoch sind, ergeben sich typischerweise hohe Anzahlen zu beurteilender Zustandskombinationen. Jedoch bestehen aufgrund des systematischen Aufbaus der BN-Modelle Möglichkeiten zur Aufwandsreduktion und Verbesserung der praktischen Handhabung, was in dem darauffolgenden achten Kapitel im Zuge der Ergebnisdiskussion näher dargestellt wird. In diesem Kapitel wird zunächst die grundlegende methodische Umsetzung prinzipiell untersucht.

7.1.2 Berücksichtigung von Fehlern gemeinsamer Ursache (Common Cause)

In den Veröffentlichungen zur Fehlermodellierung mit BN wird allgemein vorausgesetzt, dass stochastische Abhängigkeiten durch entsprechende Berechnungsalgorithmen im Netzwerk kompensiert werden. Konkrete Untersuchungen und Charakterisierungen diesbezüglich gibt es jedoch bislang jedoch nicht. Abgesehen von einzelnen Anmerkungen bezüglich Fehlern gemeinsamer Ursache [Portinale99, Bobbio01, Mahadevan01] sind bislang keine ausführlicheren Betrachtungen probabilistischer Abhängigkeiten in Werken zur BN-Zuverlässigkeitsmodellierung verfügbar.

Fehler gemeinsamer Ursache werden vereinfachend als Fehler gemeinsamer Ursache bezwiehungsweise synonym als CC-Fehler (englisch „common cause failures“) bezeichnet. Diese sind definiert als „Fehler mehrerer Bestandteile, die aus einer einzelnen Ursache resultieren, die üblicherweise als voneinander unabhängig eingestuft werden würden“ (übersetzt aus dem Englischen) [IEC60050-192:15]. Anders als im Fall von Kaskadenfehlern folgen diese mehrfachen Folgen nicht schrittweise kausal aufeinander, sondern treten jeweils für sich von der gemeinsamen Ursache ausgehend auf. In [Portinale99, Bobbio01] wird eine Möglichkeit zur Berücksichtigung von Fehlern gemeinsamer Ursachen vorgeschlagen, wobei jedoch keine probabilistische Abhängigkeit modelliert wird, sondern vereinfachend eine Anpassung der Ausfallwahrscheinlichkeit einer jeweiligen Komponente.

In [Bobbio01] wird vorgeschlagen, die Funktionswahrscheinlichkeit von Verbundkomponenten um einen pauschalen Korrekturfaktor für CC-Fehler zu mindern. Dadurch wird eine Wahrscheinlichkeit dafür berücksichtigt, dass ein Komponentenverbund ausfallen kann, obwohl dessen Unterkomponenten fehlerfrei arbeiten. In [BfS-Schr-37:05] wird dementgegen ausgehend von realen Beobachtungen in Kernkraftwerken geraten, keine pauschalen Werte für Ausfälle gemeinsamer Ursache anzunehmen, da dies in den dort behandelten Fällen zu einer systematischen und deutlichen Unterschätzung geführt hätte. Nach [BfS-Schr-37:05] kann sich dies in der Form von Sekundärdefekten und kommandierten Fehlern auswirken. Diese wurden zuvor in diesem Kapitel bereits dargestellt.

Daher wird hier vorgeschlagen, die probabilistische Abhängigkeit als Beziehung vom ursächlichen Knoten auf die jeweils betroffenen Knoten im BN-Fehlermodell abzubilden.

Im Unterschied hierzu beschreibt [Mahadevan01] die Modellierung von CC-Fehlern als gesonderte Einflussgrößen in BN. Diese werden an jeweils zutreffender Stelle in das BN-Fehlermodell angeknüpft. Dabei ist das Modell kein hierarchisches Integralmodell, sondern repräsentiert die logischen Gatter eines zugrundeliegenden Fehlerbaums. Nachfolgend wird in Kapitel 7.7 eine zu [Mahadevan01] analoge Zuordnung von CC-Fehlern zum Systemmodell diskutiert, jedoch im Unterschied dazu in Bezug auf das Mehrzustands-Fehlermodell nach dem in dieser Arbeit behandelten integralen Aufbauprinzip.

7.1.3 Probabilistische Berücksichtigung von Fehlerreaktionsmechanismen

In der Sicherheitstechnik im fachlichen Kontext der funktionalen Sicherheit [IEC61508:10] sind Sicherheitsnachweise zu erbringen, für die unter anderem probabilistische Abschätzungen auf Basis der Wahrscheinlichkeiten von Fehlerursachen mit sicherheitskritischen Folgen notwendig sind. Dabei ist die Unterscheidung zwischen potenziell gefährlichen und ungefährlichen Folgen sowie die Diagnose und Fehlerreaktion zur Gefahrenabwehr speziell relevant. Hierbei ist zudem zu berücksichtigen, dass die Fehlerreaktion typischerweise eine Unzuverlässigkeit aufweisen kann. Durch diese würde sie mit einer gewissen Wahrscheinlichkeit bei Bedarf nicht wirksam sein. Dieser Effekt wird in Form des sogenannten Diganosedeckungsgrads (englisch: „diagnostic coverage factor", DC) [IEC61508:10] beziffert.

In [Lampis09] wird beschrieben, dass auch die Fehlerwahrscheinlichkeit von überwachender Sensorik eines Systems im BN-Fehlermodell darstellbar ist. Dies geschieht dort jedoch ausschließlich anhand binärer Zuverlässigkeitsmodelle, mit den dualen Zuständen {*‚Funktion', ‚Ausfall'*}. Differenzierungen spezifischer Folgen aufgrund verschiedener möglicher Fehlzustände der Detektion und deren Auswirkungen im Zusammenhang mit Systemfunktionen erfolgen dort nicht. In [Kaiser15] wurde ein weitergehender Ansatz für eine Modellierung von Fehlererkennungs- und Fehlerreaktionsmechanismen in probabilistisch erweiterten FMEA-Fehlernetzen gezeigt. Dies wird erreicht, indem die Wahrscheinlichkeit der Funktionsfähigkeit als reduzierender Faktor mit einer potenziell gefährlichen Folge verbunden modelliert wird. Hierzu wird sowohl der Faktor DC berücksichtigt, als auch die Folgen eines unangebrachten Auslösens des Sicherheitsmechanismus, sowie dessen anzunehmende Unwirksamkeit durch einen Fehler in diesem selbst. Analog dazu wird in Kapitel 7.5 gezeigt, wie dieses Schema zur probabilistischen Modellierung spezifischer Fehlerfolgen und des Diagnosedeckungsgrads DC auch in integralen BN-Fehlermodellen darstellbar ist.

7.2 Strukturhierarchisches Systemmodell

Anhand der eingangs zusammengefassten Randbedingungen und der in den vorangegangenen Abschnitten dieser Arbeit ausgearbeiteten Grundlagen kann ein methodischer Ansatz zum Aufbau von strukturhierarchischen Mehrzustands-Fehlermodellen im beispielhaften Rahmen von BN definiert werden. Die Systemstruktur richtet sich dabei grundlegend nach dem strukturhierarchischen Aufbau des Systems, wie in Bild 7.1 dargestellt ist.

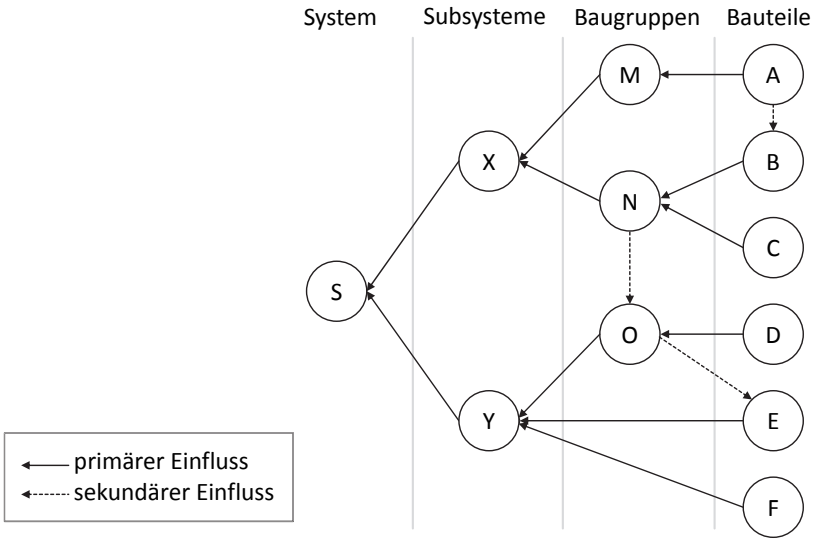


Bild 7.1: Schema eines strukturhierarchisch gegliederten Fehlermodells eines Systems

Durch das Schema eines strukturhierarchisch gegliederten Inferenznetzwerks (s. Kapitel 4) können die Einflüsse der Unterkomponenten aus probabilistischer Perspektive anhand von bedingten Wahrscheinlichkeiten aussagenlogisch einem jeweils davon abhängigen Folgezustand des Komponentenverbunds zugeordnet werden.

Auf der strukturell detailliertesten Ebene, der Ebene der Bauteile, sind in erster Linie unabhängige Zufallsgrößen angeordnet. In diesen können sich mögliche Fehlerursachen im Sinne von Primärfehlern einstellen (vgl. Kapitel 4, sowie [Vesely81]). Aus diesen wird gefolgert, welcher Fehlzustand des Verbunds im Einzelfall daraus resultiert. Jedoch können die Bauteilzustände von anderen Einflüssen abhängig sein, wenn diese mögliche Fehlzustände einnehmen, die als sekundäre oder kommandierte Fehler von anderen Ursachen provoziert werden. Die in diesen Fällen geltenden probabilistisch abhängigen Beziehungen werden als Schwerpunkt in Abschnitt 7.4 behandelt, während Erläuterungen zu unabhängigen Primärfehlern in Abschnitt 7.3 enthalten sind.

Gruppen von Bauteilen sind als Komponentenverbünde wiederum selbst Komponenten eines hierarchisch übergeordneten Verbunds. Die möglichen Fehlzustände dieser

Komponenten stellen wiederum die Ursachen für mögliche Fehlzustände des Verbunds dar. Deren Vorliegen und auch deren Kombinationen werden im gemeinsamen Folgeknoten, der den Komponentenverbund darstellt, zu dessen jeweils zutreffenden Folgezuständen logisch zugeordnet. Falls eine Ursache oder eine Kombination von Ursachen verschiedene Auswirkungen haben kann, so lässt sich mit bedingten Wahrscheinlichkeiten unterscheiden, wie wahrscheinlich die jeweils unterschiedlichen Folgezustände eintreten können. Auf diese Weise entstehen aussagenlogisch und probabilistisch konsistente strukturhierarchische Beziehungssysteme, die das Fehlermodell eines Systems wie in Bild 7.2 symbolisiert bilden.

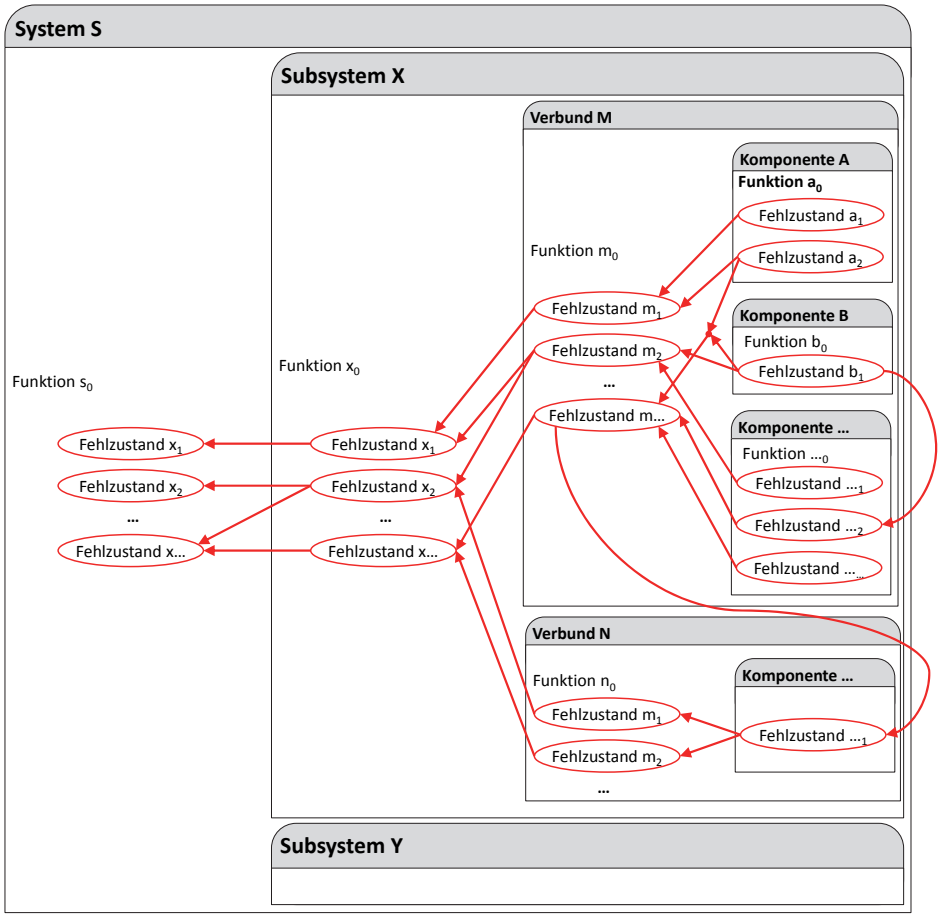


Bild 7.2 generisches Beispiel komplexer Fehlerbeziehungen in integralem Modellschema

Mittels BN lassen sich so alle eingehenden Zustände der Unterkomponenten miteinander in allen möglichen Zustandskombinationen gemäß deses Schemas probabilistisch darstellen sowie Folgezuständen in deren Verbund gegebenenfalls anteilig zuordnen. Diese Schritte der Kombination und Zuordnung drücken dabei logische Beziehungen aus, die sich in Anlehnung an [Pearl82] (vgl. Kapitel 2.4 und 6.1) in dazu abgewandelter Form formulieren lassen:

„Wenn A..., dann möglicherweise B..., andernfalls C..."

Für die Modellierung von Fehlerbeziehungen mittels solcher Ursache-Folge-Relationen sind neben der technologischen Aussage über die Fehlzustände, die im jeweiligen Fall geeignet abzugrenzen sind, auch deren probabilistische Beziehungen korrekt einzuordnen. Hierbei ist eine Differenzierung nach den in Kapitel 3 dargestellten Fehlerklassen nach [Vesely81] ausschlaggebend. Für den Komponentenfehler gilt, dass dieser primär, also aus der Komponente selbst heraus entsteht oder sekundär, durch eine nicht spezifikationsgemäße Betriebsweise der Komponente in dieser selbst provoziert wird. Zudem können kommandierte Fehler auftreten, die ein Fehlverhalten aufgrund äußerer Fehlansteuerung hervorbringen. Wie in Kapitel 4.2 bereits erörtert wurde, sind primäre Fehler probabilistisch unabhängig. Sekundäre Fehler hingegen werden bedingt durch die Wahrscheinlichkeit der Ursache der Betriebsweise ausserhalb der Spezifikation. Gleiches gilt für kommandierte Fehler. Die jeweils geeignete Modellierungsstrategie im Kontext der integralen Fehlermodelle wird in den nachfolgenden Kapiteln behandelt.

7.3 Probabilistisch unabhängige Primärfehler

Primärfehler stellen die ursächlichen Fehlerquellen dar, die in einem Bauteil selbst auftreten können. Sie sind die Grundlage für resultierende Fehlerwahrscheinlichkeiten im Modell. Daher berücksichtigt die Modellierung solche Fehler in der jeweils betrachteten Komponente, die dort unter den gegebenen Betriebsbedingungen aus dem Bauteil heraus heraus auftreten können. Im Kontext der hierarchisch übergeordneten Ebene, dem Komponentenverbund, werden dessen mögliche Folgen identifiziert. Dies wiederum ist der Fehlzustand, den der Bauteilverbund als Komponente betrachtet dann einnehmen wird, wenn diese konkrete Ursache vorliegt. Der Fehlzustand des Verbunds wiederum wird darauffolgend als Ursache für mögliche Fehlzustände des hierarchisch übergeordneten Komponentenverbunds zugrundegelegt (s. Bild 7.2). Dieses Prinzip, welches in Kapitel 4 in das Rahmenkonzept eingeflossen ist, entspricht dem Grundansatz der Fehlermodelle der FMEA. Aus den Fehlzuständen der Basiskomponenten, typischerweise der Bauteile, werden dadurch auf Grundlage von den möglichen Ursache-Wirkungs-Beziehungen schrittweise die daraus ausgelösten Fehlzustände des Systems abgeleitet.

Weist ein Bauteil einen Fehler auf, können andere Bauteile mitunter deren Funktionsweise nicht korrekt ausprägen. Der Betriebszustand dieser Bauteile ist von der Funktion der primär fehlerhaften Komponente mit betroffen, sodass dieses daher selbst Abweichungen gegen-über der vorgesehenen Funktionsweise aufweisen. Da diese in dem Fall jedoch nicht defekt sind, sind sie funktional und somit auch probabilistisch abhängig. Es handelt sich dabei um einen Sekundärfehler beziehungsweise einen kommandierten Fehler.

In Bild 7.3 ist die entsprechende Anschauung schematisch dargestellt. Darin ist beispielsweise ein Fehler eines Sensors die Ursache dafür, dass eine zu starke Ansteuerung eines Elektromotors zu einer fehlerhaft zu hohen Versorgungsspannung an dem Motor führt. Dies ruft in der Folge ein zu hohes Drehmoment hervor. So sind Motor und Regler im Beispielfall selbst nicht defekt, obwohl sie dennoch nicht die geforderte Funktion aufrechterhalten können.

Die Wirkung des Fehlers, die sich innerhalb der Hierarchieebene betrachtet fortpflanzt, ist jedoch eine Konsequenz des ursächlichen Fehlers. Es liegen jedoch keine weiteren ursächlichen, primären Fehler vor. Die übrigen Komponenten verhalten sich ihrer Spezifikation entsprechend, während sie die fehlerhafte Betriebsweise zwangsläufig auf Basis ihrer regulären Eigenschaften umsetzen.

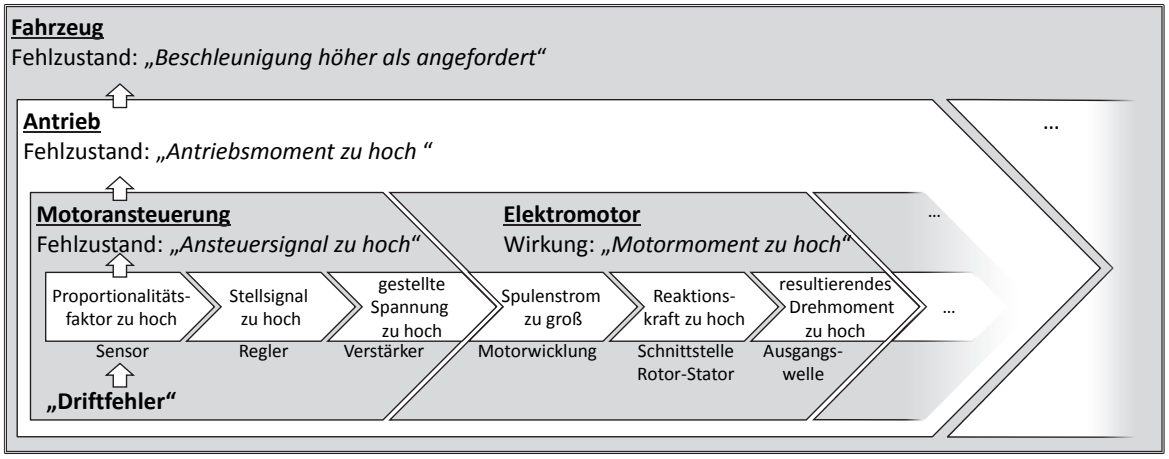


Bild 7.3: Veranschaulichung der strukturhierarchisch orientierten Interpretation von Fehlzuständen (vertikale Pfeile) auf Basis resultierender Fehlerwirkungen (horizontale Pfeile)

In diesem Fall ist es aufgrund der strukturhierarchischen Abstraktion nicht zweckmäßig, die gesamte funktionale Propagation der Fehlzustände durch alle Bauteile hindurch darzustellen, was der Wirkungskette in horizontaler Richtung in Bild 7.3 entspricht. Dies kann dagegen im strukturhierarchisch aufgebauten BN-Fehlermodell in bestimmten Fällen die Wahrscheinlichkeit gemeinsamer Folgen fälschlich erhöhen, wenn bedingt unabhängige Folgekomplexe darin enthalten sind (vgl. Kapitel 5). Ausnahmefälle jedoch, in welchen dies dennoch zweckdienlich ist, werden im folgenden Abschnitt zu probabilistisch abhängigen Fehlern behandelt.

So erfolgt die Betrachtung von Ursache und Wirkung stattdessen typischerweise auf Basis primärer Fehler und deren Auswirkungen als Fehlzustände des Komponentenverbunds. Die Fehlzustände der einzelnen Komponenten, die ebenfalls von der Fehlerwirkung betroffen sind und daher nicht ordnungsgemäß funktionieren können, werden dabei durch die Symptomatiken auf den übergeordneten Hierarchieebenen ausgedrückt.

7.4 Probabilistisch abhängige Fehler innerhalb des Systems

Neben den unabhängigen Primärfehlern gibt es wie zuvor erwähnt auch solche Fehler, deren Eintreten von der Wahrscheinlichkeit anderer abhängt (vgl. Kapitel 5). Dies sind sekundäre Defekte und kommandierte Fehler (vgl. Kapitel 4). Solche sekundäre Folgedefekte können beispielsweise weitere Folgekomplexe hervorrufen, die sich aus technologischer Sicht bedingt unabhängig voneinander verhalten können. Dies bedeutet, der sekundäre Schaden und dessen spezifische Folgewirkung entwickeln sich probabilistisch unabhängig, also parallel zu den Auswirkungen des Primärdefekts, nachdem dieser eintritt und den sekundären Schaden provoziert. Dies ist von den individuellen Gegebenheiten abhängig und muss anhand des technologischen Verhaltens entsprechend beurteilt werden. Auch kann die primäre Ursache ausserhalb des Systems liegen. Die Fehlerwirkungen beziehungsweise Defekte der betroffenen Komponenten im System sind dabei ein möglicher Ausgangspunkt für Komplexe aus Fehlerfolgen im System, während sie von einer Ursache ausserhalb des Systems abhängen. Solche probabilistischen Abhängigkeiten können demnach entweder auf einem primären ursächlichen Fehler im System oder auf einem Fehler ausserhalb des Systems beruhen. Solche Einflussbeziehungen stellen zusätzliche probabilistische Einflüsse im Netzwerk dar. Dies muss als zusätzliche Netzwerkbeziehung im strukturhierarchischen Modell abgebildet werden.

7.4.1 Sekundärdefekte

Nach der Definition der Sekundärdefekte (s. Kapitel 4.3) gilt dies für Schädigungen und Funktionsstörungen, die im Fall von nicht spezifizierten Betriebsbedingungen und Einwirkungen entstehen. Geht man von einem System aus, dessen Auslegung auf einer angemessenen Spezifikation im Sinne des Rahmenkonzepts (vgl. Kapitel 4) beruht, so kann ein sekundärer Defekt nur in solchen Fällen auftreten, in welchen ein primärer Defekt oder ein kommandierter Fehler die Ursache einer Abweichung vom spezifizierten Betrieb darstellen. Der Sekundärdefekt kann als dessen Folge eintreten. Im Fall von Fehlerkaskaden wiederholt sich dieser Vorgang als Verkettung sich sukzessive auslösender Defekte.

Solche Sekundärdefekte ziehen als Folge eines primären Defekts möglicherweise zusätzliche und gegebenenfalls kritischere Effekte nach sich. Diese verhalten sich funktional im Sinn einer bedingten Unabhängigkeit, da von dieser eine eigene kausale Usache-Folge-Beziehung ausgeht, sobald sie vom Primärfehler verursacht wurden. Daher sind diese probabilistisch relevant und müssen im Fehlermodell abgebildet werden.

Anhand des Beispielsystems aus dem vorigen Unterkapitel kann ein möglicher Ansatz, wie in Bild 7.4 dargestellt, zur Modellierung eines Kaskadenfehlers verdeutlicht werden. Gesetzt den Fall, der Sensor würde einen Fehlerfall „Kurzschluss“ aufweisen, so würde dies den Regler zum Stellen der maximalen Ausgangsleistung veranlassen und eine konstante Ansteuerung des Motors mit vollem Spulenstrom bewirken. Neben der zwangsläufigen maximalen Beschleunigung des Fahrzeugs ergäbe sich dabei eine unangemessen hohe elektrische und dadurch thermische Belastung der Motorspulen. Im Beispielfall könnte ein thermisch bedingter Ausfall des Motors folgen, der eventuell eine kritische Überhitzung nach sich zieht.

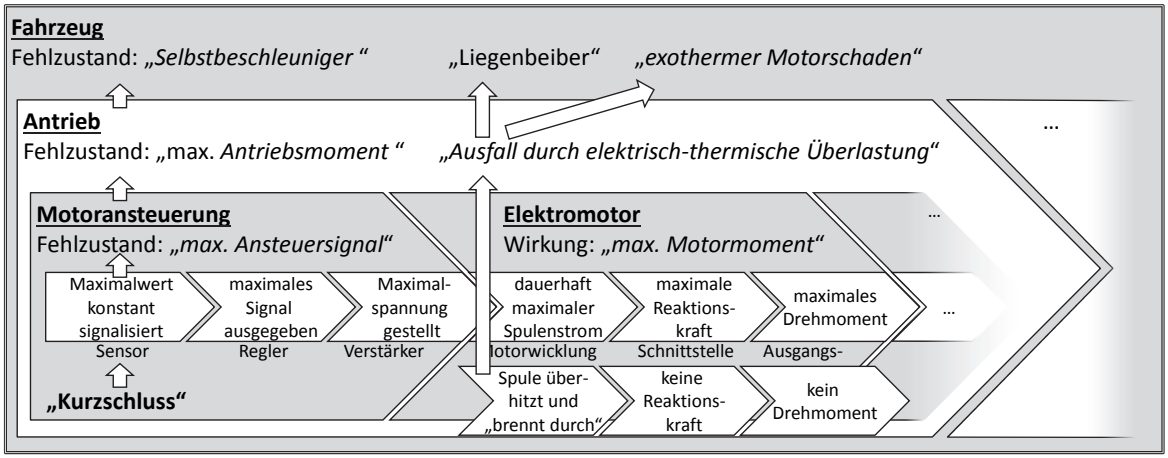


Bild 7.4: Schema eines Sekundärfehlers im Kontext des hierarchischen Systemaufbaus im Vergleich zum primären Fehler in Bild 7.3

Die Umsetzung dieser Fehlerbeziehungen im BN erfolgt in dem in Kapitel 6 erläuterten Abhängigkeitsschema für bedingt unabhängige Fehlerauswirkungen. Deren Grundschema ist in Bild 7.5 anhand einzelner beispielhaft symbolisierter Fehlerbeziehungen dargestellt. Ein entsprechendes Fehlermodell in Form eines BN wird in Bild 7.6 gezeigt.

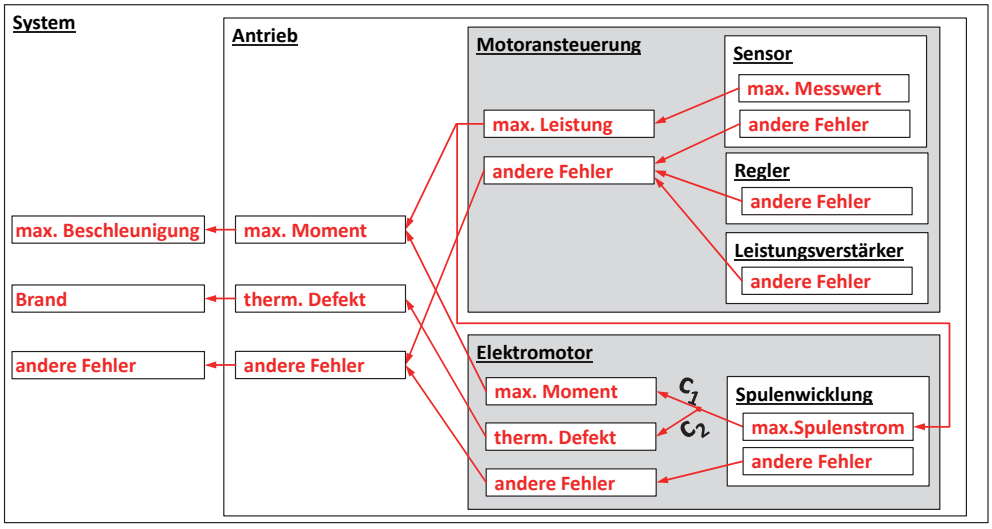


Bild 7.5: symbolische Darstellung der Beziehungen eines Sekundärdefekts (s. Bild 7.4)

In dem Beispielnetzwerk in Bild 7.6 wurden der spezifische Sensorfehler, die konstant maximale Motoransteuerung sowie der sich dadurch konstant einstellende maximale Spulenstrom mit der Folge des maximalen Motormoments berücksichtigt. Zur Verbeserung der Übersichtlichkeit des Beispiels sind einzelne unspezifische Fehlzustände als „andere Fehler" angegeben. Die den sekundären Fehler bewirkende Beziehung wurde zwischen den Knoten „Motoransteuerung" und „Spulenwicklung" angeordnet, da diese die Fehlansteuerung des Motors auslöst.

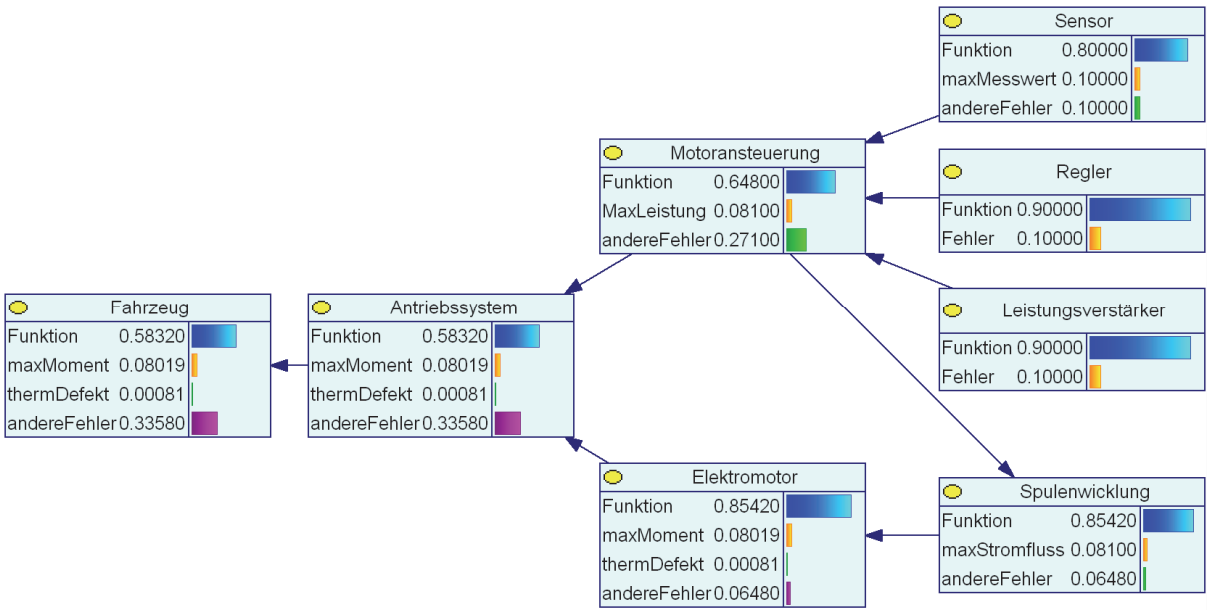


Bild 7.6: BN zum Beispiel eines Kaskadenfehlers als bedingt unabhängige Folgewirkung

Zu einem probabilistisch identischen Ergebnis gelangt man ebenso, indem die Einflussbeziehung zwischen Sensor und Spulenwicklung modelliert wird, wie rechts in Bild 7.7 dargestellt ist. Diese jedoch richtet sich nicht nach dem hierarchischen Modellschema, das im Sinne des funktionalen Verständnisses des Rahmenkonzepts geeigneter ist, um solch ein System zu repräsentieren.

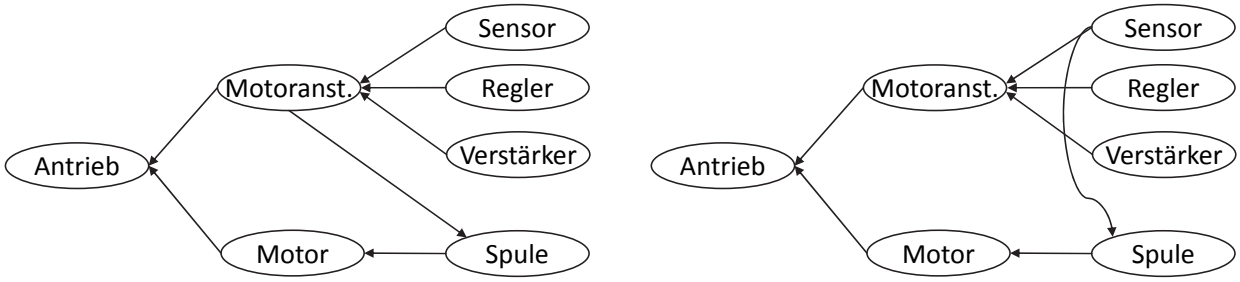


Bild 7.7: alternative Modellstrukturen für das Anschauungsbeispiel (vgl. Bild 7.4).

7.4.2 Kommandierte Fehler

Bei der Fehlerklasse der kommandierten Fehler handelt es sich um ein fehlerhaftes Verhalten einer Komponente, ohne dass diese selbst einen Fehler aufweist. Diese zeigt aufgrund von fehlerhafter oder zur Unzeit erfolgender Ansteuerung ein unvorgesehenes Verhalten (vgl. Kapitel 4.2.2). Dies wird beispielsweise auch in FTA-Untersuchungen betrachtet [Vesely81].

Kommandierte Fehler können in gleicher Weise wie Kaskadenfehler im BN-Modell repräsentiert werden. Hierbei ist zu beachten, dass die primäre Fehlerursache an anderer Stelle als Voraussetzung vorliegen oder ausgelöst werden muss. Der kommandierte Fehler ist davon zum einen probabilistisch abhängig und kann daher zur Wahrung der probabilistischen Konsistenz nicht als unabhängiger Fehler angegeben werden. Zum anderen ist wie im Fall sekundärer Fehler darauf zu achten, dass dieser nicht implizit bereits in den Fehlerbeziehungen des Modells enthalten ist. Andernfalls besteht die Möglichkeit, dass eine fälschliche Überhöhung der resultierenden Folgewahrscheinlichkeit im Modell durch darin enthaltene bedingt unabhängige Folgebeziehungen auftritt, obwohl dies in diesem Fall nicht dem realen Verhalten entspricht.

7.4.3 Fehler gemeinsamer Ursache

Wie bereits in Kapitel 7.1 erläutert, sind Fehler gemeinsamer Ursache solche Fehlerphänomene, in welchen ein ursächlicher Konflikt davon abhängige Fehlerfolgen an mehreren Stellen im System provoziert. Dies kann sowohl durch eine äußere schädigende Einwirkung oder eine Wirkung von einer Quelle im Systeminneren verursacht sein, die sich schädigend auf mehrere andere Stellen im System auswirkt. Da CC-Fehler durch eine Ursache mehrere Folgen auslösen, besteht hier eine wie in Kapitel 6.4 beschriebene bedingte Unabhägigkeit zwischen diesen Folgen.

Das Modellierungsschema stellt sich anhand eines Beispiel aus [BfS-Schr-37:05] wie in Bild 7.8 veranschaulicht dar. Bei dem Beispielsystem geht es um eine redundante Möglichkeit zur Absperrung eines Durchflusses. Die Redundanz besteht aus zwei verschiedenen Ventilen, die entlang der Durchflussleitung in Reihe geschaltet sind. Beide Ventile sind von derselben elektrischen Versorgung abhängig, sodass deren Ausfall einen Fehler gemeinsamer Ursache für beide Ventile darstellt. Fällt die Versorgung aus, so kann die Leitung bei Bedarf nicht gesperrt werden. Dies wird in dem Fehlerbaum nach [BfS-Schr-37:05] (Bild 7.8, links) sowie in dem RBD (Bild 7.8, rechts) dargestellt.

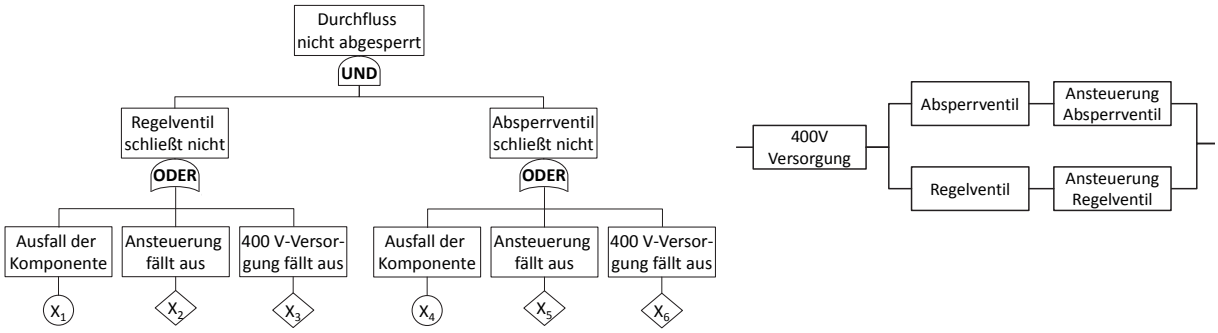
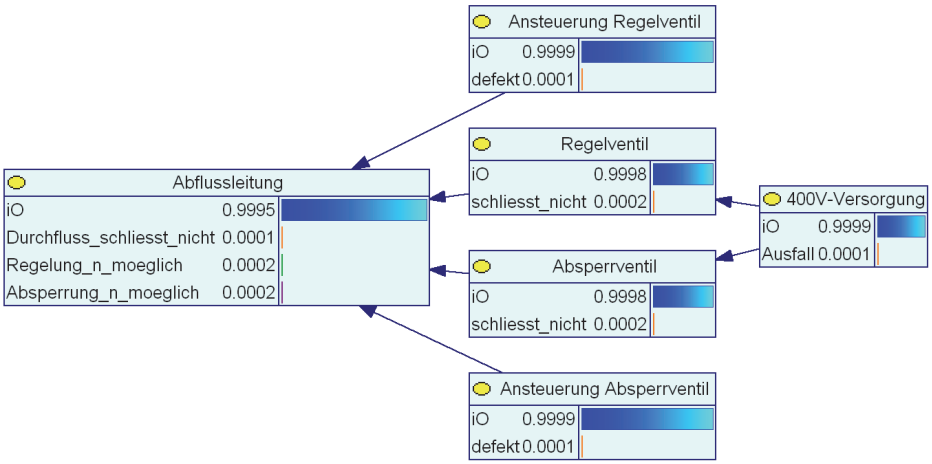


Bild 7.8: Fehlerbaum nach [BfS-Schr-37:05] für den kommandierten, anhängigen Ausfall der Absperrung des Durchflusses (links); Darstellung als RBD (rechts)

Dieses Fehlermodell kann wie in Bild 7.9 und 7.10 dargestellt in Form eines hierarchischen BN unter Berücksichtigung weiterer System-Fehlzustände konsistent berechnet werden.



CPT: Regelventil

400V-Versorgung	i.O.	Ausfall
i.O.	0,9999	0
schliesst nicht	0,0001	1

CPT: Absperrventil

400V-Versorgung	i.O.	Ausfall
i.O.	0,9999	0
schliesst nicht	0,0001	1

Bild 7.9: BN-Fehlermodell des Beispiels nach [BfS-Schr-37:05] mit Implementierung des CC-Fehlers durch den Ausfall der elektrischen Versorgung in den CPT der Ventile

CPT: Abflussleitung

Ansteuerung Regelventil	i.O.								defekt							
Regelventil	i.O.				schliesst nicht				i.O.				schliesst nicht			
Absperrventil	i.O.		schliesst nicht		i.O.		schliesst nicht		i.O.		schliesst nicht		i.O.		schliesst nicht	
Ansteuerung Absperrventil	i.O.	defekt	i.O.	defekt	i.O.	defekt	i.O.	defekt	i.O.	defekt	i.O.	defekt	i.O.	defekt	i.O.	defekt
i.O.	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Durchfluss schliesst nicht	0	0	0	0	0	1	1	1	0	1	1	1	0	1	1	1
Regelung n. möglich	0	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0
Absprrenung n. möglich	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0

Bild 7.10: CPT des Knotens „Abflussleitung“ in Bild 7.9

Die Wahrscheinlichkeit für primäre Fehler wurde für beide Ventile implementiert, unter der Bedingung, dass die Versorgungsspannung zur Verfügung steht. Im Fall des Ausfalls der elektrischen Versorgung wurde die Folgewahrscheinlichkeit mit 1 angegeben. Im CPT des Knotens „Abflussleitung“ (s. Bild 7.10) wurde unterschieden, ob die jeweilige Zustandskombination entweder zu einem Funktionsausfall des Regelventils oder des

Absperrventils führt. Alle Zustandskombinationen, in welchen beide Ventile ausgefallen sind beziehungsweise nicht mehr angesteuert werden, wurden der Folge „Durchfluss schließt nicht" zugeordnet. Die resultierenden Wahrscheinlichkeiten beruhen auf fiktiven Werten von $P(\text{‚}Ausfall\text{‘}) = 1 \cdot 10^{-4}$ für alle Fehlerursachen.

7.5 Probabilistischer Einfluss durch Fehlerreaktion des Systems

Insbesondere sicherheitsrelevante Systeme können spezifische Funktionen enthalten, die im Fall eines Fehlers einer Basiskomponente, typischerweise eines elementaren Bauteils, diesen erkennen und spezifische Reaktionen zur Kompensation oder Minderung unerwünschter Auswirkungen auslösen können. Dazu werden Fehlzustände, die potenziell zu gefährlichen Auswirkungen führen, durch entsprechende Funktionen des Systems zur Selbstdiagnose detektiert. Um den zu vermeidenden Auswirkungen zu begenen, werden fallabhängig mildernde Gegenmaßnahmen ausgelöst oder Warnsignale ausgegeben. Die Intervention des Fehlerreaktionsmechanismus beeinflusst den Aufbau des Fehlermodells und die damit errechneten Zustandswahrscheinlichkeiten. Das charakteristische Schema dieser Zusammenhänge auf Basis von Fehlerreaktionsmechanismen ist in Bild 7.11 veranschaulicht.

Ein konkretes Beispiel dafür ist eine automatische Abschaltung eines Systems, die ausgelöst werden soll, bevor gefährliche Konsequenzen eintreten können. Eine erfolgreiche Abwendung gefährlicher Folgen wird je nach Systemkonzept beispielsweise durch ungefährliche Fehlerfolgen erreicht, indem das System beispielsweise durch eine Abschaltung in einen sicheren Zustand versetzt wird. In dem Fall wird das Fehlernetz durch eine probabilistisch wirksame Fehlerreaktion erweitert, da deren Eingreifen die Wahrscheinlichkeit der Folgen beeinflusst. Die Realisierung einer solchen Fehlerreaktion erfodert jedoch in der Regel den Einsatz zusätzlicher Komponenten, die selbst wiederum eine potenzielle Fehlerquelle mit spezifischen Auswirkungen darstellen.

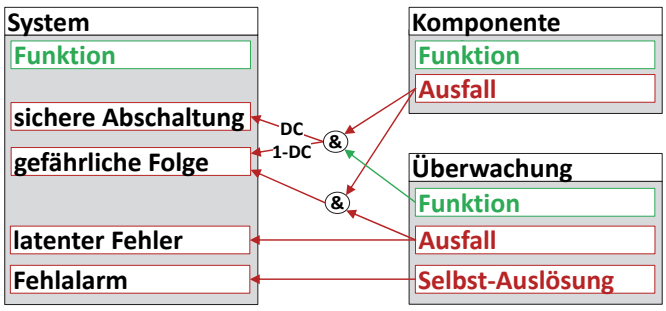
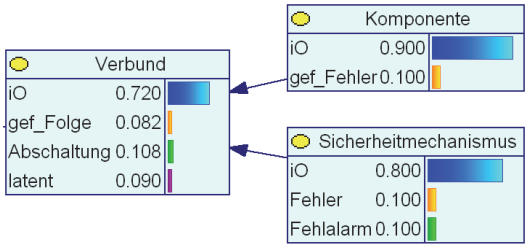


Bild 7.11: Schema ausgewählter probabilistischer Fehlerbeziehungen zwischen diagnostizierter und diagnostischer Funktionseinheit nach [Kaiser15]

Wie in Abschnitt 7.1 bereits erwähnt, können solche Beziehungskomplexe nach [Kaiser15] in einem Fehlermodell probabilistisch ausgedrückt werden. Dies lässt sich in analoger Weise auch im integralen Ansatz zur Fehlermodellierung mit BN darstellen. Hierzu sei jedoch erwähnt, dass die nachfolgende Betrachtung sicherheitsrelevanter Fehlerbeziehungen und diesbezüglicher Systemreaktionen in probabilistischen Fehlermodellen in dieser Arbeit sich ausschließlich auf die Modellierung der Komponentenzustände und deren probabilistischen Beeinflussungen bezieht. Für eine korrekte Verwendung in konkreten Sicherheitsnachweisen muss dies im gegebenen Kontext plausibilisiert und nachgewiesen werden. Zudem ist die Berechnungsgrundlage gegenüber den Anforderungen an den Nachweis zu verifizieren.

Durch die Funktion des Sicherheitmechanismus soll erreicht werden, dass der potenziell kritische Fehler nicht zu einer gefährlichen Folge führt. Stattdessen wird dies durch eine geeignete Gegenmaßnahme unterbunden. Die Wahrscheinlichkeit, dass dies erfolgreich geschieht, wird durch den Diagnosedeckungsgrad DC ausgedrückt (vgl. Kapitel 7.1). Mit dem Anteil des komplementären Werts $(1 - DC)$ wird der gefährliche Zustand hingegen nicht erkannt beziehungsweise diesem nicht genügend wirksam begegnet, sodass sich der kritische Fehler dennoch ungehindert in ungünstiger Weise auswirken kann. Allerdings kann die diagnostische Komponente aufgrund von Fehlzuständen in ihren Unterkomponenten selbst auch Fehler aufweisen. Dies reduziert zum einen die Wahrscheinlichkeit der Funktionsfähigkeit, was die Wahrscheinlichkeit der Abwendung gefährlicher Folgen der abzusichernden Komponente mindert. Zudem ergeben sich spezifische Folgen aus den Fehlzuständen der überwachenden Komponente.



	i.O.			gefährlicher Fehler		
Verbund	**i.O.**	**Fehler**	**Fehlalarm**	**o.k.**	**Fehler**	**Fehlalarm**
i.O.	1	0	0	0	0	0
ges. Folge	0	0	0	0,9	1	0
Abschaltung	0	0	1	0,1	0	1
latent	0	1	0	0	0	0

Bild 7.12: BN-Modell zur Berücksichtigung der Beeinflussung eines Komponentenfehlers durch einen Sicherheitsmechanismus (links) und CPT (rechts)

So können zwei typische Arten von Folgen durch Fehler des Mechanismus zur Fehlerreaktion auftreten. Dies ist zum einen ein sogenannter latenter Ausfall [IEC61508:10, ISO26262:11]. In diesem Fall führt ein Fehler in der Diagnosefunktion dazu, dass diese im Bedarfsfall nicht funktionsfähig ist und daher nicht wie vorgesehen eingreifen kann. Ein Grund dafür kann es sein, dass die Detektion des Fehlers nicht erfolgt oder die Erkennung zwar stattfindet, die Fehlerreaktion jedoch nicht auslösbar ist. Die andere typische Möglichkeit für Fehler durch

solche Fehlerreaktionsmechanismen ist die einer fälschlichen Auslösung. In dem Fall wird eine Fehlerreaktion beziehungsweise ein Fehlalarm ausgelöst, ohne dass der gefährliche Fehler tatsächlich gegeben ist. Bild 7.12 stellt die Implementierung aller zuvor geschilderten Zusammenhänge zwischen der zu überwachenden Komponente und dem Sicherheitsmechanismus als integrales BN-Fehlermodell beispielhaft dar. Die durch die Parameter in der CPT zu implementierenden Zustansdzuordnungen beruhen dabei auf dem generischen Schema möglicher Zustandskombinationen, das in Bild 7.13 symbolisiert ist. Darin überlagern sich die Zustände der Zufallsgrößen „Komponente“ K, als der zu überwachende Systemteil, und „Überwachung“ D, als die überwachende Einheit, innerhalb des überwachten Systembestandteils M.

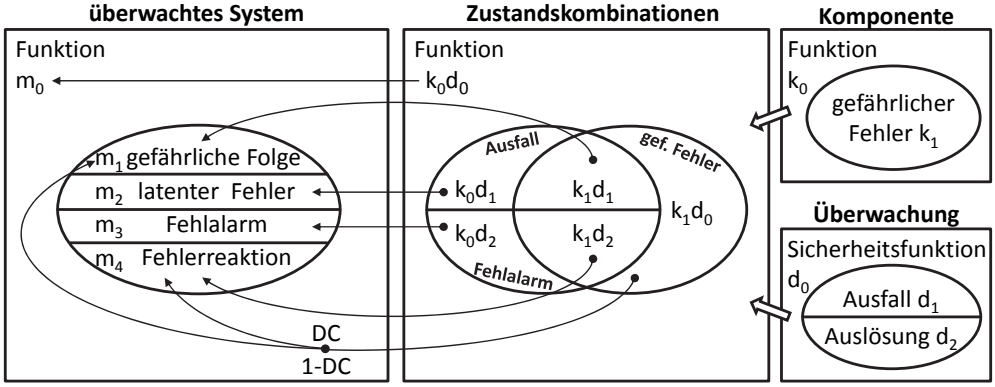


Bild 7.13: Überlagerung der Zustände von Komponente und Sicherheitsmechanismus sowie deren Zuordnung zu resultierenden Folgezuständen des Komponentenverbunds

Tritt eine Kombination aus dem gefährlichen Fehler der überwachten Komponente und des Sicherheitsmechanismus auf, können zudem unterschiedliche Folgen angenommen werden, je nach dem, welcher Fehler zuerst auftritt. Reihenfolgen der Vorkommnisse der Fehler werden in dem hier diskutierten Fehlermodell nicht differenziert. Daher beruht die Wahrscheinlichkeit eines Doppelfehlers auf der Sichtweise, dass beide Fehler zu beliebigen Zeitpunkten innerhalb der Zeitspanne der Betrachtung aufgetreten sein können. Dazu muss berücksichtigt werden, dass ein Fehler in der Regel zunächst einzeln vorliegt, bevor der andere hinzukommt.

Liegt im Betrachtungszeitraum zuerst der potenziell gefährliche Zustand der Komponente vor, ohne dass der Ausfall des Sicherheitsmechanismus zuvor eingetreten ist, so kann die SIcherheitsfunktion wie vorgesehen ausgelöst werden. Umgekehrt jedoch, wenn der latente Fehler vorliegt, bevor der gefährliche Fehlzustand der Komponente auftritt, kann dieser sich ungehindert gefährdend auswirken. Für die Zustandskombination aus Komponentenfehler latentem Fehler ist es daher zwecks defensiver Einschätzung nötig, den schwerwiegenderen

zweiten Fall im Modell zu berücksichtigen und somit die gefährliche Folge als resultierenden Effekt anzugeben.

Für die Kombination aus Komponentenfehler und Fehlalarm ist das fälschliche Auslösen die kritischsere der anzunehmenden Konsequenzen. Diese muss im vereinfachten Modell für diese Fehlerkombination als defensive Annahme getroffen werden. Dies leitet sich aus den möglichen Ereignsikombinationen ab. Tritt nämlich als erstes der gefährliche Komponentenfehler ein, so ist davon auszugehen, dass der Sicherheitsmechanismus, seine Aufgabe der Diagnose und Fehlerreaktion unmittelbar erfüllt. Die Annahme eines nachfolgenden fälschlichen Auslösen des Sicherheitsmechanismus im Sinne eines Fehlalarms ist in diesem Fall obsolet. Tritt hingegen zunächst die fälschliche Aktivierung des Sicherheitsmechanismus ein und zu einem späteren Zeitpunkt der gefährliche Komponentenfehler, wurde diesem unbeabsichtigt bereits vorauseilend begegnet, was dann kein falsches Auslösen mehr darstellen würde. Mit der pauschalen Annahme der Konsequenz des fälschlichen Auslösens ist dieser Komplex von Kombinationsmöglichkeiten somit hinreichend dargestellt im Sinne der defensiven Einschätzung möglicher Folgen.

7.6 Probabilistische Abhängigkeit von äußeren Einflüssen

Für die Fehlermodellierung eines Systems ist mitunter auch die Berücksichtigung probabilistischer Einflüsse ausserhalb des Systemgrenzen von Interesse. Dabei muss jedoch berücksichtigt werden, welche Einflüsse bereits in den Daten der Fehlerwahrscheinlichkeiten einzelner Bauteile berücksichtigt sind, da diese grundsätzlich auf konkreten Betriebsrandbedingungen beruhen. Davon abweichende Zustände und Einflüsse können gegebenenfalls ergänzend zur Fehlzustandswahrscheinlichkeit der Bauteile in das Systemmodell einbezogen werden.

Als spezifisch zu modelliernde Einwirkungen auf das Modell kommen solche in Betracht, die Fehler mit der Charakteristik sekundärer beziehungsweise kommandierter Fehler hervorrufen können (s. Kap. 3 und [Vesely81]). Sind mehrere Bauteile hiervon betroffen, stellt dies zudem einen CC-Fehler dar können (s. Abschnitt 7.4.3). Solche äußeren Primärfehler können als Netzwerkknoten zusätzlich zum BN-Modell des Systems modelliert werden. Deren Einfluss auf die Kindknoten, also typischerweise die elementaren Bauteile des Systems, machen für diese die Unterscheidung der Fehlerwahrscheinlichkeiten nötig, im Falle des regulären Betriebs ohne diese Einwirkung, sowie der Fehlerwahrscheinlichkeit, wenn die Einwirkung gegeben ist.

7.7 Topologisch bedingte Abhängigkeiten

Die Implementierung von Redundanzen wurde bereits bei [Bobbio01] für BN-Fehlermodelle im Stil des dort genutzten Modellierungsprinzips gezeigt. In [Portinale15] wird die Möglichkeit der Umsetzung in systemhierarchischen Mehrzustandsmodellen grundsätzlich vorgeschlagen, was jedoch nicht konkret untersucht wurde. Dies geschieht nachfolgend im Einzelnen in Bezug auf integrale BN-Fehlermodelle.

7.7.1 Redundanz mit mehrwertigen Zufallsgrößen

In Abschnitt 7.4.3 wurde bereits eine solche Redundanz gezeigt (vgl. Bild 7.8). In dem dort dargestellten Fall kann die betreffende Funktion der Absperrung des Durchflusses durch eines der beiden Ventile erreicht werden. In der zughörigen CPT wurde die durch die Reihenschaltung der Absperrventile realisierte Redundanz im BN modelliert, was in Analogie zu dem ursprünglichen Beispiel in [BfS-Schr-37:05] jedoch in binärer Weise erfolgte. Darüber hinaus sind jedoch auch Mehrzustands-Komponenten in entsprechender Weise darstellbar.

Ein anschauliches Beispiel nach [VDA-Band4:03] kann zur Darstellung von Redundanz in einem Mehrzustands-Fehlermodell angeführt werden. Dieses beschreibt eine Maschinenwelle, die zwecks Redundanz zwei Freilaufkupplungen K_1 und K_2 enthält (vgl. Bild 7.14 a). Für diese Komponenten werden je zwei Fehlzustände unterschieden. Die beiden identischen Freilaufkupplungen können in dem Beispiel jeweils den Fehler ‚bricht' aufweisen, wodurch die Übertragung unterbrochen ist.

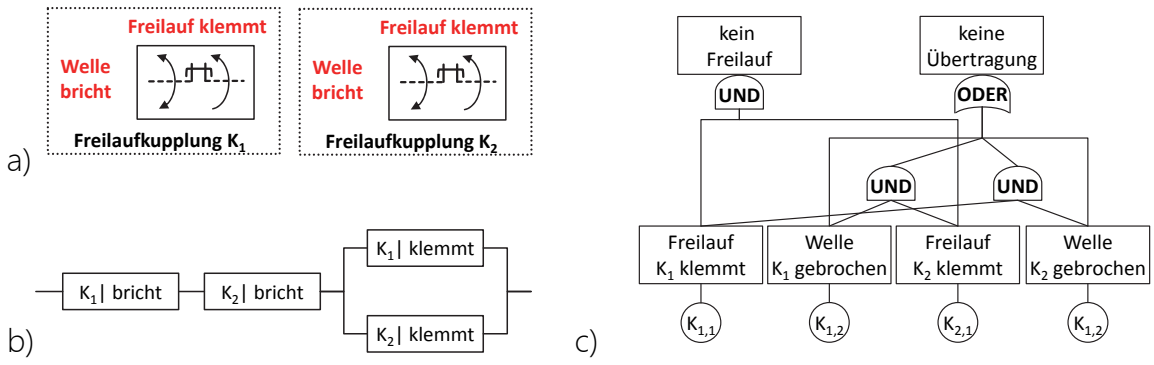


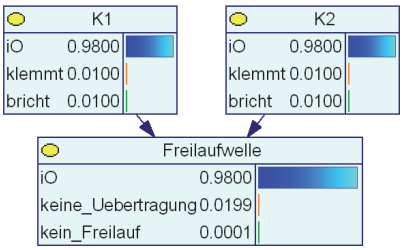
Bild 7.14: Beispiel nach [VDA-Band4:03] einer Welle mit doppeltem Freilauf (a) mit RBD (b) und Fehlzustandsdiagramm im Stil eines Fehlerbaums (c)

Der Fehlzustand ‚klemmt' führt dazu, dass der Freilauf festgesetzt ist und daher eine starre Verbindung auch in der eigentlichen Freilaufrichtung vorliegt. Klemmt nur einer der beiden Freiläufe, so kann der andere dennoch dessen Funktion erfüllen, wodurch die Redundanz erreicht wird. Ist jedoch ein Freilauf gebrochen, so erfolgt keine Momentübertragung über

die Welle. Diese Serienschaltung der Funktionen der Momentübertragung sowie die Redundanz durch die zweifache Freilauffunktion werden durch das Zuverlässigkeitsblockdiagramm nach Bild 7.14 b) repräsentiert. Zudem lassen sich die Folgen möglicher Fehlzustandskombinationen mit logischen Notationselementen in Anlehnung an die FTA wie in Bild 7.14 c) gezeigt modellieren. Diese stellt die komplexen Abhängigkeiten und Kombinationsmöglichkeiten dieser Anordnung dar. Eine konsistente und exakte Auswertung ist mit den für RBD und FTA gebräuchlichen Berechnungsansätzen aufgrund der stochastischen Abhängigkeiten nicht mehr ohne weiteres möglich. Mit dem zuvor in dieser Arbeit diskutierten Ansatz ist dies jedoch konsistent und exakt darstellbar und berechenbar.

In einem strukturhierarchisch integralen BN-Fehlermodell können die möglichen Zustände dieser Baugruppe implementiert werden. Im Unterschied beispielsweise zu [Zhou06] ist dabei keine Unterteilung anhand des RBD und dessen Umsetzung in mehereren Operatoren-Knoten erforderlich. Mit zufällig gewählten Zahlenwerten für Fehlerwahrscheinlichkeiten ergeben sich für das integrale BN-Modell (vgl. Bild 7.15) beispielsweise diese Wahrscheinlichkeitsverteilungen:

$$P(K_1) = P(K_2) = \begin{bmatrix} P('in\ Ordnung') \\ P('klemmt') \\ P('bricht') \end{bmatrix} = \begin{bmatrix} 0{,}98 \\ 0{,}01 \\ 0{,}01 \end{bmatrix}$$



Freilauf K_1	i.O.			klemmt			bricht		
Freilauf K_2	i.O.	klemmt	bricht	i.O.	klemmt	bricht	i.O.	klemmt	bricht
i.O.	1	1	0	1	0	0	0	0	0
keine Übertragung	0	0	1	0	0	1	1	1	1
kein Freilauf	0	0	0	0	1	0	0	0	0

Bild 7.15: BN-Fehlermodell der Welle mit doppeltem Freilauf (links) [GeNIe10] und CPT (rechts)

Es besteht eine probabilistische Abhängigkeit aufgrund der Exklusivität der Zustände der mehrwertigen Zufallsgrößen K_1 und K_2. K_1 beziehungsweise K_2 können jeweils entweder im Zustand eines der Fehlermodi {‚*klemmt*' } und {‚*bricht*' } ausgefallen sein, beziehungsweise sich andernfalls im Zustand {‚*kein Fehler*'} befinden. Dies wird, wie in Kapitel 5 erläutert, in der Berechnung des BN korrekt berücksichtigt.

Rechnet man mit den gebräuchlichen Formeln für Serien- und Parallelschaltung in RBD nach Gleichung (2.15, 2.16), ohne den gegenseitigen Ausschluss der Zustände der Komponenten

zu berücksichtigen, ergibt sich mit $P(\text{‚}kein\ Fehler\text{‘}) = 0{,}98000199$ ein mit rund $0{,}2$ ‰ geringfügig abweichendes Ergebnis. Um dies zu überprüfen kann die gegenseitige Exklusivität der Fehlermodi {‚*klemmt*‘} und {‚*bricht*‘} jeweils in K_1 und K_2 auch im BN-Fehlermodell ausser Acht gelassen werden. Modelliert man dazu die Fehlzustände der Freiläufe in unabhängigen Knoten jeweils separat (s. Bild 7.16), erhält man dieselbe Abweichung von dem korrekten Ergebnis. Da diese ergänzende Berechnung unter Vernachlässigung der Exklusivität der Zustände jedoch probabilistisch nur näherungsweise korrekt ist, werden die Gleichungen und CPT-Parameter nicht ausdrücklich angegeben.

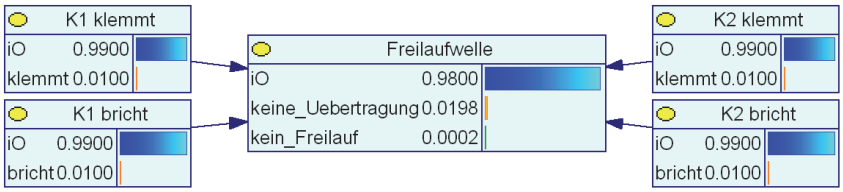


Bild 7.16: Berechnung des Beispiels mit unkorrekter Annahme der Unabhängigkeit der jeweiligen Zustände {‚*klemmt*‘} und {‚*bricht*‘} der Freilaufwellen K_1 und K_2 [GeNIe10]

Ein weiterer erwähnenswerter Punkt liegt in der Kombinatorik der Zustände der Komponenten. Durch die Bildung aller möglichen Zustandskombinationen im CPT des Knotens „Freilaufwelle“ sind dort auch Kombinationen zu bewerten, die zwar probabilistisch betrachtet korrekt sind, technologisch jedoch in der Form nicht zwangsläufig plausibel beziehungsweise möglich sind. So gibt es die Kombination des Bruchs beider Kupplungen. Die Fehlerkombination bezeichnet die Wahrscheinlichkeit, dass innerhalb des Betrachtungszeitraums beide Komponenten zu beliebigen Zeitpunkten diesen Fehler erleiden. Jedoch ist anzunehmen, dass nach einem Bruch im Lastpfad durch die gesamte Welle hindurch kein zweiter Bruch möglich ist, da sich die dazu notwendigen Belastungen nicht mehr einstellen können. In diesem Anschauungsbeispiel ist davon auszugehen, dass nach Bruch in einer der Kupplungen der Fall des endgültigen Verlusts der Kraftübertragung, also der Ausfall der Welle, mit entsprechenden Konsequenzen für das System eintritt.

Ähnliche Problematiken wurden bereits auch im Unterkapitel zu Fehlerreaktionen im Bezug auf die Reihenfolge des Fehlereintretens diskutiert. Im gegebenen Einzelfall ist zu beurteilen, welcher Folge die Wahrscheinlichkeit eines Zustands zugeordnet wird. Dies sollte anhand der Überlegung möglicher Eintretensreihenfolgen und zeitlicher Abstände zwischen den Ereignissen spezifisch beurteilt werden sowie unter Berücksichtigung möglicher Konsequenzen. Im Zweifel ist dies der kritischeren Folge zuzuordnen. Fallweise kann auch eine Aufteilung der Zustandswahrscheinlichkeit auf die verschiedenen jeweils möglichen Auswirkungen plausibel sein.

7.7.2 Mehrzustands-Zuverlässigkeit bei kumulativen Funktionen und Pseudo-Redundanz

In ähnlicher Weise, wie die Berücksichtigung der Mehrzustands-Zuverlässigkeit im Kontext unmittelbarer Redundanz, können auch Zuverlässigkeitsbetrachtungen mit Teilredundanzen (Pseudoredundanz) erfolgen. So kann beispielsweise ein einzelner Ausfall oder Fehler eines der Systemteile nicht den völligen Ausfall des Systems bewirken, dessen Leistungsfähigkeit oder aber dessen Funktionsfähigkeit jedoch eingeschränkt ist. Ansätze zu probabilistischen Betrachtungen der Abstufung der Leistungsfähigkeit von Systemen finden sich unter anderem in [Aven99, Misra08, Lisnianski10, Natvig11].

Die Möglichkeiten, dies in einem integralen strukturhierarchischen BN-Fehlernetz zu behandeln, kann an dem Beispiel eines Verkehrsflugzeugs mit vier Triebwerken veranschaulicht werden. Dieses Luftfahrzeug benötigt den Schub aller Triebwerke für Start und anfänglichen Steigflug. Für den weiteren Flug wird jedoch nicht mehr der volle Schub aller Triebwerke zwingend benötigt, was auch in der Zuverlässigkeitsbetrachtung berücksichtigt werden kann. Für das Beispiel gelte, es genüge der Schub von dreien der vier Triebwerke für einen uneingeschränkten Flugbetrieb nach Erreichen der Reiseflughöhe und ebenso für eine sichere, eventuell vorgezogene Landung. Zudem seien zwei Triebwerke für einen hinreichend kontrollierbaren Flug und eine Notladung genügend, solange sich die ausgefallenen Triebwerke nicht an derselben Tragfläche befinden.

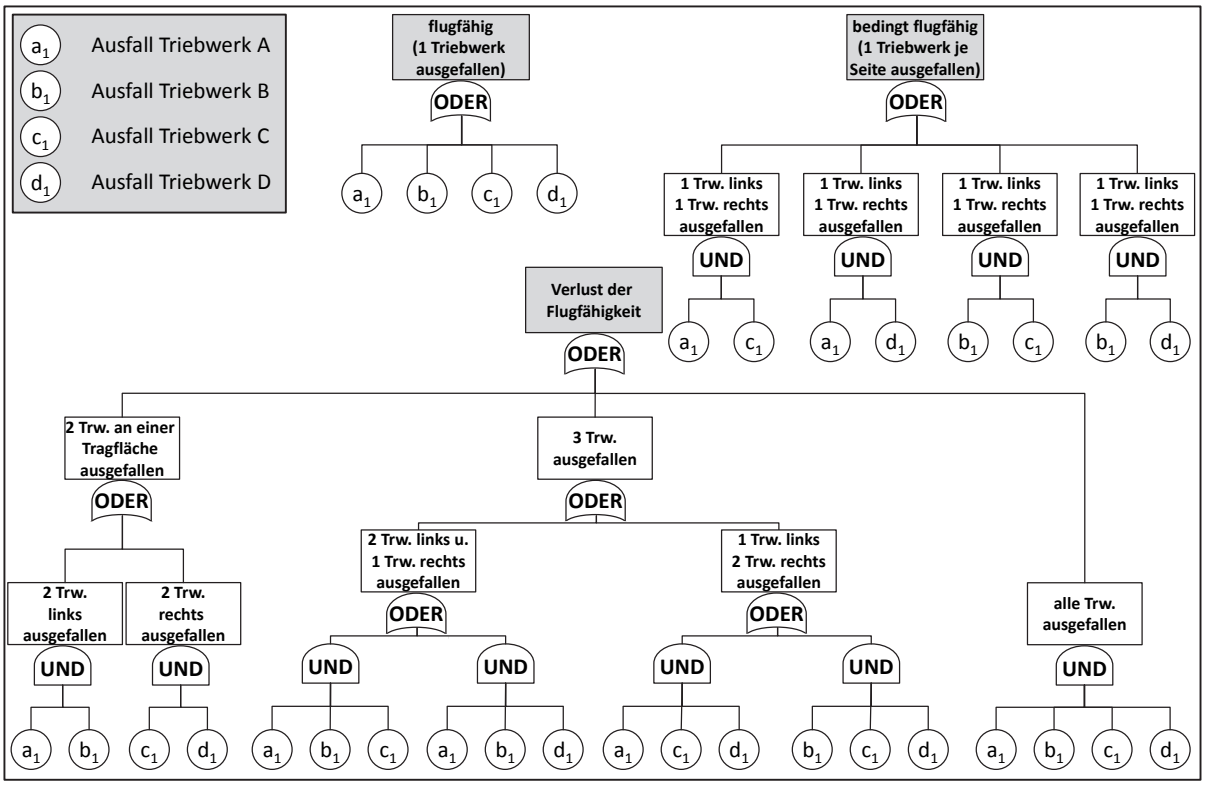
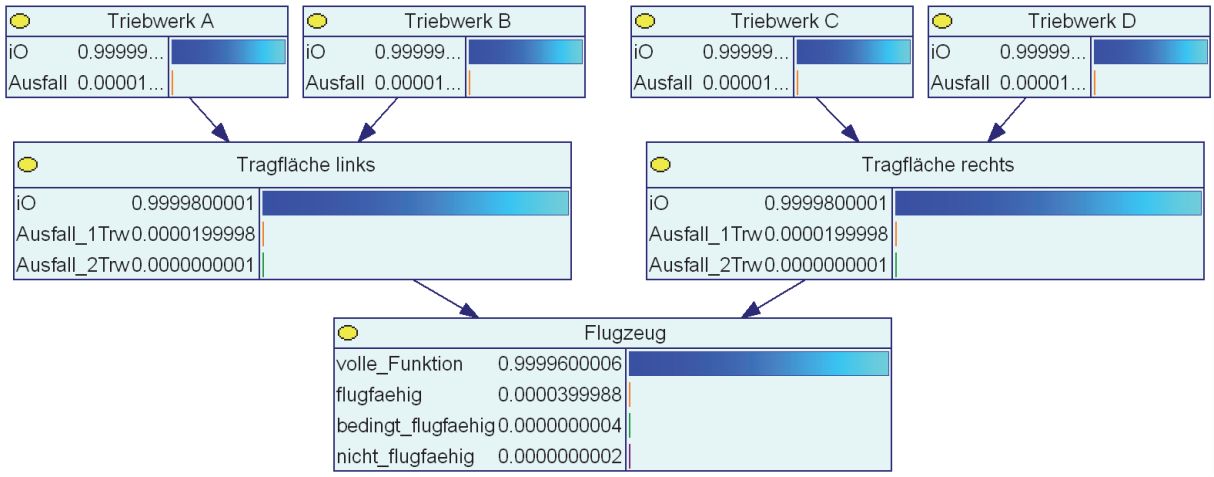


Bild 7.17: FT für das Beispiel: ‚Triebwerksausfälle einer vierstrahligen Verkehrsmaschine'

In Bild 7.17 sind Fehlerbäume für drei Szenarien dargestellt. Der Zustand {*‚flugfähig'*} gelte bei Ausfall eines Triebwerks, was nach der Startphase im Rahmen des Beispiels keine unmittelbaren Komplikationen bedeutet. {*‚bedingt flugfähig'*} liege im dem Fall des Versagens zweier Triebwerke an verschiedenen Tragflächen vor, wodurch ein Weiterflug und eine gut beherrschbare Landung möglich seien. Der Fall {*‚flugunfähig'*} bezeichne das Versagen zweier Triebwerke an derselben Tragfläche, oder aber dreier beziehungsweise aller vier Triebwerke. In diesen Fällen sei von einem schadenfreien Ausgang des Flugs nicht hinreichend gewiss auszugehen. Die Ausfälle der Triebwerke werden zur Vereinfachung als voneinander unabhängig angenommen. Fehler gemeinsamer Ursache bleiben hier vereinfachend zugunsten der Prägnanz des Beispiels unberücksichtigt. Triebwerk A und B befinden sich gemeinsam an einer Tragfläche, C und D an der anderen.



CPT: Tragfläche links

Triebwerk A	i.O.		Ausfall	
Triebwerk B	i.O.	Ausfall	i.O.	Ausfall
i.O.	1	0	0	0
Ausfall 1 Trw.	0	1	1	0
Ausfall 2 Trw.	0	0	0	1

CPT: Tragfläche rechts

Triebwerk C	i.O.		Ausfall	
Triebwerk D	i.O.	Ausfall	i.O.	Ausfall
i.O.	1	0	0	0
Ausfall 1 Trw.	0	1	1	0
Ausfall 2 Trw.	0	0	0	1

CPT: Flugzeug

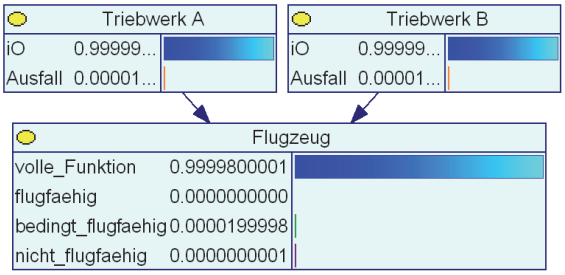
Tragfläche links	i.O.			Ausfall 1 Trw.			Ausfall 2 Trw.		
Tragfläche rechts	i.O.	Ausf. 1 Trw.	Ausf. 2 Trw.	i.O.	Ausf. 1 Trw.	Ausf. 2 Trw.	i.O.	Ausf. 1 Trw.	Ausf. 2 Trw.
volle Funktion	1	0	0	0	0	0	0	0	0
flugfähig	0	1	0	1	0	0	0	0	0
bedingt flugfähig	0	0	0	0	1	0	0	0	0
nicht flugfähig	0	0	1	0	0	1	1	1	1

Bild 7.18: strukturhiarchisches BN-Fehlermodell ‚Triebwerksausfälle einer vierstrahligen Verkehrsmaschine' in [GeNle10] (oben); zugehörige CPT (mitte und unten)

Bild 7.18 stellt das dem Beispiel entsprechende BN-Fehlermodell bestehend aus dem Netzwerk und den zu den Knoten gehörigen CPT dar. Die verwendeten Zahlenwerte wurden für das Beispiel zufällig gewählt und basieren auf der Annahme einer Wahrscheinlichkeit für den Ausfall eines Triebwerks während eines zehnstündigen Fluges $P_{10h} = 10^{-5}$.

Erwähnenswert ist zudem, dass bei diesem Modellierungsprinzip nicht anhand der Ausfallreihenfolge differenziert wird (s. auch 7.5 und 7.7.1). Daher sind die Zahlenwerte in der Weise zu interpretieren, dass sich diese jeweils auf den Endzustand beziehen, der sich innerhalb der betrachteten Zeitspanne einstellt. Bei Ausfallkombinationen ist daher auch anzunehmen, dass diese zeitlich versetzt eintreten können. Dies schließt beispielsweise den Fall ein, dass innerhalb der Flugdauer sich zunächst ein Ausfall ereignet und weitere Triebwerksausfälle unabhängig vom ersten zu einem zufälligen Zeitpunkt während der restlichen Flugdauer hinzukommen. Die Differenzierung dieser Fälle zur Berücksichtigung der Ausfallreihenfolge erscheint ferner analog zu [Boudali04, Weber06] als zeitdiskreteisertes Verfahren beziehungsweise [Boudali06, Marquez10] als kontiunierliches Berechnungsmodell möglich. Diese dort gezeigten Verfahren lassen sich ebenfalls in dem hier vorgeschlagenen Modellierungsansatz implementieren, was jedoch hier nicht weiter vertieft wird.

Abschließend wird zum Vergleich die Berechnung der Zustandswahrscheinlichkeiten einer zweistrahligen Maschine links in Bild 7.19 abgeschätzt. Dies erfolgt unter der Annahme, dass die Maschine bei Ausfall eines Triebwerks noch zu einer beherrschbaren Notlandung gebracht werden kann, jedoch nicht mehr als grundsätzlich flugfähig eingestuft wird. Dies wird anhand der Verteilungen der bedingten Wahrscheinlichkeiten in der CPT implementiert (s. Bild 7.19 rechts). Für die beiden Triebwerke wurde dabei die gleiche Ausfallwahrscheinlichkeit, wie im vorangegangenen Beispiel angenommen. So ergibt sich hierfür eine geringere Wahrscheinlichkeit für völlige Flugunfähigkeit x_3 sowie eine höhere Wahrscheinlichkeit für Fehlerfreiheit x_0 als für die zuvor untersuchte vierstrahlige Maschine.



Triebwerk A	i.O.		Ausfall	
Triebwerk B	i.O.	Ausfall	i.O.	Ausfall
volle Funktion	1	0	0	0
flugfähig	0	0	0	0
bedingt flugfähig	0	1	1	0
nicht flugfähig	0	0	0	1

Bild 7.19: BN-Modell einer zweistrahligen Verkehrsmaschine in [GeNIe10] (links); CPT der zur Berechnung implementierten bedingten Wahrscheinlichkeiten (rechts)

8 Ergebnisdiskussion

Eine objektive Beurteilung der Ergebnisse analytischer Methoden zur Fehleranalyse unterliegt einem grundsätzlichen Dilemma, da die reale Verifikation von Fehlermodellen anhand statistisch aussagekräftiger Daten für komplexe Gesamtsysteme de facto nicht möglich ist. Hierfür müsste eine entsprechend umfassende Datenbasis durch immense Versuchsaufwände oder aus Betriebsdaten ermittelt werden, um alle im Fehlermodell behandelten Fehlzustände und Fehlerkombinationen im Versuch statistisch nachzuweisen. Nichtsdestotrotz gilt es nach dem Stand von Wissenschaft und Technik als plausibel und valide, davon auszugehen, dass die aussagenlogische Repräsentation und Bewertung eine prinzipiell geeignete und in ihrer Eigenschaft als modellhafte Abstraktion korrekte Grundlage für Fehlermodelle darstellt. Ausgehend von dieser grundsätzlichen Hypothese der Gültigkeit der Fehlermodellierung auf Basis probabilistischer Zusammenhänge kann ein relativer Vergleich zwischen methodischen Ansätzen erfolgen. So erfolgt die Ergebnisbewertung in Form einer Charakterisierung der Methodik hinsichtlich speziell relevanter und wichtiger Aspekte im Vergleich zu anderen Methoden beziehungsweise allgemein auf qualitative Weise.

8.1 Vergleich mit anderen Methoden

Der Grundansatz der hier diskutierten integralen BN-Fehlermodelle ist prinzipiell vergleichbar zu solchen der klassischen FTA und RBD. So stellen die berechneten Wahrscheinlichkeiten Erwartungswerte des Vorliegens der Zustände am Ende eines betrachteten Zeitraums dar. Durch die Untersuchungen in dieser Arbeit konnte gezeigt werden, dass die Berechnung im Prinzip dieselben Ergebnisse hervorbringt wie die etablierten quantitativen Verfahren, sofern die Modelle dieselben logischen Strukturen aufweisen. Dabei bietet die integrale BN-Fehlermodellierung jedoch aufgrund der Abbildbarkeit bedingter Folgemöglichkeiten einerseits eine erhöhte Präzision des Modells durch die realistischere Abbildung von Folgenmöglichkeiten gegenüber den Ansätzen zur Mehrzustands-Fehlermodellierung, da keine Näherung auf Basis seltener Ereignisse (vgl. [Vesely81]) zur Auswertung verwendet wird.

Die Fehlerbeziehungen im strukturhierarchisch orientierten BN-Fehlermodell weisen vordergründige Ähnlichkeiten zur FMEA auf. Zwar enthält die FMEA keine Kombinationen von Fehlermöglichkeiten und keine bedingten Folgewahrscheinlichkeiten, jedoch stellen beide die Beziehung zwischen Fehlerursache und Fehlerfolge in hierarchisch funktionalem Sinn dar. Die Modelle unterscheiden sich dagegen prinzipiell in der Hinsicht voneinander, dass in der FMEA jedem Fehlzustand beliebig viele Fehlerfolgen zugeordnet werden können. Dabei

muss nicht unterschieden werden, ob diese Folgen zugleich oder aber alternativ zueinander auftreten. Im probabilistisch integralen Fehlermodell muss stattdessen eine eindeutige Ursache-Wirkungs-Beziehung spezifiziert werden. So kann stets nur eine Folge modelliert werden beziehungsweise mehrere alternative Folgen, die sich gegenseitig ausschließen. Gleichzeitig mögliche Zustände können nicht als verschiedene diskrete Zustände der übergeordneten Komponente angegeben werden. Dies ist aufgrund der logischen und arithmetischen Grundlage notwendig, da das Integralmodell gegenseitig exklusive probabilistische Zustände beinhaltet. Für die ausschließlich qualitative FMEA ist die Beschränkung hingegen nicht notwendig und nicht definiert, da keine arithmetische Randbedingung für probabilistische Integrität herrscht. So ist es mitunter ein Ziel der FMEA, möglichst viele zutreffende Folgezustände an eine Fehlerursache anzuknüpfen, um ein vollständiges Spektrum möglicher Folgeeffekte angeben zu können. Der integrale Ansatz der BN-Fehlermodellierung kann dies hingegen nicht in gleicher Weise abbilden. Stattdessen ist es notwendig, jeweils sich gegenseitig ausschließende Folgezustände zu beschreiben, wie dies in Kapitel 6.3 erläutert wird.

Die Einbeziehung der probabilistischen Möglichkeiten (aus dem Englischen „likelihood“) für alternative Auswirkungen stellt dabei jedoch keinen Konflikt zur probabilistischen Grundlage der Ursache-Wirkungs-Modelle dar (vgl. Abschnitt 5.2 sowie [Pearl00, Jaynes03]). Vielmehr handelt es sich um eine arithmetische Verfeinerung innerhalb der Randbedingung, dass zur Erhaltung der probabilistischen Integrität des Modells nur alternative Folgen durch bedingte Wahrscheinlichkeiten ausgedrückt werden können. Die bei der Berechnung der Netzwerke erfolgende Kompensation von stochastischen Abhängigkeiten kann als eine weitere Präzisierung des probabilistischen Verfahrens angesehen werden.

So bietet die BN-Fehlermodellierung eine verfeinerte Abbildung, als dies mit den klassischen und binären Methoden darstellbar ist, deren gröberes Modell und üblichen Approximationen der Lösungsverfahren vorwiegend die Tendenz zur Überschätzung der Wahrscheinlichkeiten der Fehlerfolgen birgt [Epstein05]. In selteneren Fällen erfolgt allerdings auch deren Unterschätzung. Nach Epstein gilt diese Problematik nicht für exakte Berechnungsverfahren, mit welchen auch die BN-Fehlermodelle ausgewertet werden können. Allerdings bietet die verfeinerte Differenzierung zwar ein differenzierteres und potenziell genaueres Modellabbild. Dies impliziert zugleich aber auch einen geringeren unwillkürlichen Sicherheitsfaktor, als die gröbere Modellierung anhand klassischer Verfahren. So ist es im Fall von Ungewissheit bezüglich der angenommenen Daten, ratsam, potenziell kritische Ursachen und bedingte Folgewahrscheinlichkeiten grundsätzlich mit höheren Werten zu bewerten.

Die Implementierung zeitlicher Bedingungen wurde in dem in dieser Arbeit vorgestellten grundlegenden Verfahren nicht eingehend betrachtet. Für eine eingehendere probabilistische und funktionale Differenzierung kann dies jedoch relevant sein und so den entsprechenden Mehraufwand bei der Modellierung rechtfertigen. Hierfür sei auf erweiterte Berechnungsverfahren zur Modellierung von Abfolgen, analog zu Ansätzen zur Zuverlässigkeitsbetrachtung auf Basis dynamischer BN verwiesen, wie beispielsweise in [Boudali04, Boudali06, Weber06, Marquez10]. Die Umsetzung des hier behandelten integralen BN-Fehlermodells in entsprechend zeitabhängiger Form ist grundsätzlich möglich.

8.2 Erkenntnisse hinsichtlich der praktischen Verwendung als Analysemethode

Im Hinblick auf die praktische Verwendung des in der Arbeit untersuchten integralen Ansatzes zur Fehlermodellierung leitet sich eine Reihe von Fragestellungen aus den Erfahrungen und Erkenntnissen der voranstehenden Ausarbeitungen ab. Diese betreffen den Umgang mit Ungewissheit, sowie Möglichkeiten zur Aufwandsreduktion bezüglich der typischerweise zahlreichen zu definierenden bedingten Wahrscheinlichkeiten in Form der CPT-Parameter und zur selektiven Beschränkung auf spezifische Analyseziele oder Systemteile.

8.1.1 Handhabung und Aufwand

Insbesondere die fallweise sehr hohe Anzahl an Parametern in den CPT der Netzwerkknoten stellt ein Hemmnis für die Umsetzung dar. Doch ist dies weniger der Methode selbst geschuldet, sondern vielmehr der Natur der Problematik der Zustandsbewertung eines Systems mit vielen zusammenwirkenden Bauteilen und jeweils mehreren möglichen Fehlzuständen. Demnach beruht die Probabilistik eines Systems stets auf diesen möglichen Konstellationen. Dies kommt aufgrund des systematischen Ansatzes, der der BN-Fehlermodellierung zugrunde liegt, notwendigerweise zum Vorschein.

Um dem zu begegnen, werden nachfolgend verschiedene Ansätze für eine Aufwandsminderung aufgezeigt. Des Weiteren dienen diese auch dazu, die Nachvollziehbarkeit und praktische Anwendung der kontextbezogen anschaulichen Gestaltung von CPT zu unterstützen. Diese Ansätze stellen einen Ausgangspunkt für eine anwendungsgerechte Umsetzung des Verfahrens, beispielsweise in dafür zu entwickelnden Anwendungsprogrammen, dar.

- *Parameterelimination anhand der Fehlerordnung:*

Je nach Anzahl der Komponenten, die in einem Verbund zusammenwirken, sowie je nach der Anzahl an potenziellen Fehlzuständen, sind mitunter große Anzahlen an Fehlerkombina-

tionen möglich. Dies sind jedoch zu einem maßgeblichen Anteil Fehlerkombinationen höherer Ordnungen (vgl. Tabelle 5.1). In der gebräuchlichen tabellarischen Darstellung der CPT werden diese typischerweise nicht entsprechend unterschieden, sodass es besonderer Bemühung bedarf, diese in deren Gesamtheit zu überblicken und irrtumsfrei zu behandeln.

Ein möglicher Ansatz ist die Priorisierung anhand der Fehlerordnung innerhalb der CPT. Fehlerkombinationen höherer Ordnungen sind in der Regel um Größenordnungen unwahrscheinlicher, als solche niederer Ordnung. So kann der Fokus beispielsweise auf die detaillierte Betrachtung von Fehlern erster Ordnung (Einzelfehler) und zweiter Ordnung (Doppelfehler) gelegt werden, während solche höherer Ordnungen pauschal ohne spezifische Zustandsbeschreibung zusammengefasst werden, was in Bild 8.1 prinzipiell veranschaulicht ist.

Fehlerordnung	**i.O.**	**Einzelfehler**							**Doppelfehler**				**Fehler höherer Ordnung**			
Verbund X		a_1	a_i...	b_1	b_j...	c_1	c_k...	...	a_ib_j	a_ic_k	b_jc_k	...	$a_ib_jc_k$	...	...	Rest
Funktion x_0																
Folge x_1																
Folge x_n																
...																
n_spez. ≥ 2.Ordnung																

Bild 8.1: Strukturierung von CPT anhand der Fehlerordnung

Bis zu welcher Fehlerordnung das Modell detailliert ausgearbeitet wird, sollte dabei beispielsweise abhängig von der Kritikalität des Systems hinsichtlich möglicher Gefährdungen für Mensch, Umgebung, Natur oder auch Sachwerte entschieden werden. Für ein nicht sicherheitsrelevantes Produkt mag es dagegen fallabhängig genügen, ausschließlich Einzelfehler explizit zu betrachten und darüber hinaus nur besonders wahrscheinliche beziehungsweise kritische Doppelfehler selektiv zu identifizieren und konkret auszuarbeiten. Da BN stets auf der Gesamtheit aller Zustandskombinationen beruhen, kann beispielsweise algorithmisch automatisiert ermittelt werden, welche der vernachlässigten Zustandskombinationen höherer Ordnung signifikante Wahrscheinlichkeitswerte aufweisen, um diese für eine spezifische Betrachtung zu selektieren.

Ergänzend kann es fallabhängig sinnvoll sein, einzelne Systemteile oder Komponentenknoten aufgrund technologischer Eigenschaften detaillierter zu betrachten, als andere. Ein Beispiel hierfür ist eine redundante Topologie in einem Systemteil. Dessen Abbildung im Modell muss bis hin zu einer Fehlerordnung geschehen, durch die alle Kombinationsmöglichkeiten der Zustände der redundanten Systemteile erfasst werden. Die ist beispielsweise die dritte

Fehlerordnung für eine sogenannte 2-aus-3-Redundanz, sodass die Wahrscheinlichkeit des Ausfalls aller drei Systemteile explizit im Fehlermodell dargestellt wird.

Ein anderes allgemeines Beispiel ist eine Sicherheitsfunktion, die bestimmten kritischen Fehlerkombinationen entgegenwirken muss. Solch ein Sicherheitsmechanismus kann, wie in Kapitel 7.5 ausgeführt ist, selbst jedoch auch Fehlzustände einnehmen, die in Kombination mit den zu verhindernden Fehlzuständen der Komponente zu beurteilen sind. Aufgrund der Sicherheitsrelevanz ist eine differenzierte Betrachtung erforderlich. Dabei sollten alle Kombinationen bis zu einer ausreichend hohen Ordnung behandelt werden, um dadurch alle Kombinationen der Fehlzustände des Sicherheitsmechanismus mit allen durch diesen zu begegnenden Zustandskombinationen der Komponente explizit abzubilden. So ist beispielsweise eine Betrachtung der Fehlerkombinationen bis zur dritten Ordnung für einen zu erkennenden Doppelfehler nötig, um die Folgen dieser Kombination bei gleichzeitigem Vorliegen eines latenten Fehlers oder Ausfalls des Sicherheitssystems abbilden zu können.

- *Parameterelemination anhand von spezifischer Einflusswirkung:*

Bei Verbindungen aufgrund probabilistischer Abhängigkeiten, beispielsweise im Fall sekundärer und kommandierter Fehler, sowie im Fall spezifisch einwirkender äußerer Einflüsse, ist eventuell nur ein bestimmter Teil des probabilistischen Einflusses betroffen. So dient es der Übersichtlichkeit, hier eine visuell optimierte Darstellung der CPT vorzusehen, die Zustände im Normalbetrieb in einer Gruppe, sowie die Einwirkungen von Sonderereignissen ein einer weiteren Gruppe zusammengefasst darzustellen (s. Bild 8.2). Auf diese Weise kann beispielsweise der Fall unter einer spezifischen Einwirkung getrennt von dem Regelfall ohne diese behandelt werden, was die Umsetzung der Analyseaufgabe vereinfacht.

		Normalbetrieb: wie spezifiziert				Sonderereignisse (Blitzschlag,Hagel,…)			
Zustände X	**P**	a_1	a_2	b_1	…	a_1	a_2	b_1	…
Funktion	1-ΣP(xi)								
Folge x_1	$P(x_1)$								
Folge x_2	$P(x_2)$								
…	P(x…)								

Bild 8.2: Strukturierung von CPT anhand regelmäßiger und besonderer Einwirkungen

- *Parameterelimination aufgrund dominanter Zustände:*

Einige Fehlzustände dominieren funktional, indem nach deren Eintreten keine anderen Zustände eintreten können beziehungsweise sich keine Veränderungen des Systemverhaltens einstellen können. Falls beispielsweise ein Fehlzustand eintritt, nach dem das System fehler-

bedingt völlig funktionslos ist, können weitere Fehlzustände keine andere Fehlerwirkung in Kombination mit diesem mehr hervorbringen und somit irrelevant sein. Diese von einem Fehlzustand dominierten Kombinationen können mitunter übergeordnet als solche gekennzeichnet und zusammengefasst behandelt werden. Durch Kennzeichnung der Dominanz eines Fehlzustands (vgl. Bild 8.3) kann dessen Auswirkung in solch einem Fall automatisch für alle weiteren Kombinationen mit diesem festgelegt werden, was wiederum die Gesamtanzahl einzeln zu betrachtender Fallunterscheidungen verringern kann.

		Einzelfehler				Doppelfehler				>2. Ordn.	
Zustände X	**P**	a_1	a_2	b_1	...	a_1b_1	a_1b_2	a_2b_1	...	...	
Funktion	$1-\Sigma P(x_i)$										
Folge x_1	$P(x_1)$	DOM	←		→	X	X			X	
Folge x_2	$P(x_2)$										
...	$P(x...)$										

Bild 8.3: Aufwandsreduktion durch Kennzeichnung dominierender Fehlzustände (dom.)

8.1.2 Umgang mit Unkenntnis, Ungewissheit und unvollständigem Wissen

Die Verfügbarkeit der für ein Fehlermodell benötigten Kenntnisse und Daten ist im praktischen Anwendungsfall beschränkt, wenn nicht alle erforderlichen Kenntnisse über Fehlzustände von Komponenten und deren Wahrscheinlichkeiten bekannt sind. Zudem mag die Einschätzung von bedingten Folgewahrscheinlichkeiten einer hohen Ungewissheit unterliegen. Dazu können diese von dem Betriebszustand und anderen Randbedingungen abhängig sein, sodass eine entsprechend komplexe Differenzierung erforderlich ist, die nicht im Modell abgebildet werden kann. Daher liegt es in der Natur der Aufgabe, die Fehlermodellierung unter vereinfachenden Annahmen und begrenzter Kenntnis umzusetzen. Dies jedoch ist ein grundsätzliches Problem der methodischen Fehleranalyse. Aus diesem Grund ist es generell zu bevorzugen, defensive Schätzungen der Wahrscheinlichkeitswerte zugrunde zu legen und die Ergebnisse in dieser Weise zu deuten. Dies kann beispielsweise dadurch geschehen, dass Abschätzungen vorrangig zugunsten von kritischen Fehlern erfolgen.

Speziell im Kontext der integralen Fehlermodellierung ist zudem zu beachten, dass die Unkenntnis möglicher Fehlerursachen oder deren Vernachlässigung zu einem höheren Wert der Funktionswahrscheinlichkeit führt, als dies tatsächlich gegeben ist. Dies liegt an der Komplementarität der Funktionswahrscheinlichkeit gegenüber der gesamten Wahrscheinlichkeit der Fehlzustände. Sind einzelne Fehlzustände nicht aufgeführt, so ergibt sich fälschlicherweise ein höherer Wert für die Funktionswahrscheinlichkeit der betreffenden Komponente.

Daher ist es für integrale Fehlermodelle insbesondere wichtig, gegebenenfalls vorhandene Einschränkungen der Kenntnisse, des Betrachtungsumfangs oder der Detaillierung der Analyse bei deren Auswertung geeignet zu berücksichtigen. Sind beispielsweise nicht alle Fehlermöglichkeiten bekannt oder im Modell implementiert, beispielsweise, um den Arbeitsaufwand zu verringern, so bietet es sich an, einen Fehlzustand „unbekannte Fehlzustände" oder „nicht spezifizierte Fehlzustände" in der Menge der Fehlzustände vorzusehen. Im Fall von Vorbehalten hinsichtlich der möglichen Fehlzustände und deren Wahrscheinlichkeiten sollten die Knoten in einer der im Folgenden vorgeschlagenen Weisen aufgebaut werden.

- *Keine Angabe der Funktionswahrscheinlichkeit:*

Falls nur spezifische Zustände betrachtet und nennenswerte Teile nicht eingehend untersucht wurden, kann keine Funktionswahrscheinlichkeit angegeben beziehungsweise ermittelt werden. In dem Fall ist es notwendig, wie in Bild 8.4 (links) dargestellt ausschließlich einen zu den behandelten Fehlzuständen komplementären Zustand „nicht spezifizierte Zustände" anzugeben, anstelle einer Funktionswahrscheinlichkeit.

Zustände X	P
nicht spez. Zustände	$1-\Sigma P(x_i)$
Folge x_1	$P(x_1)$
Folge x_2	$P(x_2)$
...	P(x...)

Zustände X	P
Funktion	$1-\Sigma P(x_i)$
Folge x_1	$P(x_1)$
Folge x_2	$P(x_2)$
...	P(...)
nicht spez. Zustände	$P(x_{Rest})$

Bild 8.4 Knotenaufbau bei nennenswerter Ungewissheit oder Vernachlässigung nicht relevanter Fehlzustände (links); Knotenaufbau bei abschätzbarer pauschaler Restfehlerwahrscheinlichkeit (rechts).

- *Angabe eines pauschalen Restfehleranteils:*

Im Fall nur einzelner unberücksichtigter oder nicht im Einzelnen bekannter restlicher Fehlermöglichkeiten, deren Größenordnung jedoch abgeschätzt werden kann, lässt sich ein nicht spezifizierter Fehlzustand angeben wie rechts in Bild 8.4 veranschaulicht. Dieser ist als Fehlzustand mit den übrigen konkret spezifizierten Fehlermöglichkeiten zusammen komplementär zur Funktionswahrscheinlichkeit. So kann diese explizit angegeben werden.

- *Selektives Modell mit Restfehler ohne Funktionswahrscheinlichkeit:*

Eine Kombination aus obigen Ansätzen ist in solchen Fällen denkbar, in welchen nur Teile des Systems näher betrachtet werden, in anderen Teilen hingegen eine grobe Differenzie-

rung möglicher Zustände oder eine weniger detaillierte Analyse genügt. Die Angabe einer Funktionswahrscheinlichkeit ist in einem solchen Fall nur abschnittsweise möglich und die Menge der ermittelten Folgen kann nicht als vollständig erachtet werden. Daher muss die Liste der Zustände eines Knotens dies entsprechend widerspiegeln, indem in den jeweiligen Komponenten, die Unterkomponenten ohne entsprechende Angaben enthalten, keine Funktionswahrscheinlichkeit angegeben wird.

Allgemein ist es für die integrale Modellierungsstrategie wichtig, dass auch für nicht ausdrücklich spezifizierte Fehlzustände angenommen werden muss, dass sich darin potenziell kritische Folgen verbergen können. Wenn diese nicht näher konkretisiert wurden oder bekannt sind, ist dies stets als potenziell kritischer Fehlerkomplex anzusehen. Zu beachten ist in diesen Fällen zudem, dass das Modell grundsätzlich nur in der Hinsicht und in dem Umfang ausgewertet und interpretiert wird, wie es angesichts der Restriktionen der verwendeten Daten und der Modellgüte angemessen ist.

8.3 Erweiterte Ansätze zur Verwendung integraler Systemmodelle

Da die Berechnung der BN-basierten Fehlermodelle mit darin enthaltenen logischen Zusammenhängen und Abhängigkeiten arithmetisch exakt möglich ist, kann die Berechnung auch mit Wahrscheinlichkeitswerten erfolgen, die nicht wesentlich kleiner als eins sind. Dies ist ein Unterschied zu der Näherung, die unter der Annahme seltener Ereignisse („rare event approximation" [Vesely81]) für die FTA vorgeschlagen wird, um Vereinfachungen der Fehlerbaum-Strukturen und Boolescher Terme zu erreichen. Hierbei besteht nicht die Notwendigkeit zur Beschränkung auf Restriktionen durch konstante Wahrscheinlichkeitswerte wesentlich kleiner als 1. Dies erlaubt es zudem, auch solche Berechnungen umzusetzen, die eine Zunahme des Wahrscheinlichkeitswerts bis hin zum Lebensdauerende abbilden, wie beispielsweise Rissbildung, Alterungseffekte und Verschleiß. Auf der Basis ist eine Berechnung des Modells unter schrittweise voranschreitender Zeit möglich, wobei erkennbar wird, zu welchem Zeitpunkt beispielsweise ein bestimmter System-Fehlzustand einen definierten Grenzwert überschreitet. Hierzu müssen Eingangswerte für die Randknoten des BN-Fehlermodells aus geeigneten Zuverlässigkeitsfunktionen der Bauteile geeignet einbezogen werden.

Als weiterführende Überlegung erscheint es ferner interessant zu sein, verschiedene Sätze von Randparametern für unterschiedliche Nutzungsszenarien und Betriebsweisen anzunehmen. Ein Konzept hierfür kann es beispielsweise sein, mehrere Konfigurationen von äußeren Einflüssen auf die Komponenten der untersten Hierarchieebene zu beziehen und die Fehler-

wahrscheinlichkeit in Abhängigkeit von diesen zu implementieren. Dabei gilt es jedoch, zu beachten, dass die Wahrscheinlichkeit eines Fehlzustands eines Bauteils beziehungsweise eines Eingangsknotens von der Beanspruchungshistorie abhängt und die individuelle Gesetzmäßigkeit zur Akkumulation der Fehlerwahrscheinlichkeit zu geeignet zu implementieren ist.

Als Überleitung zu Schluss und Ausblick der Arbeit sei noch ein Gedanke erwähnt, der es gestattet, das hier diskutierte arithmetische Konzept zur Fehlermodellierung in einer freieren Form anzuwenden. So ist es denkbar, die Fehlerbeziehungen nicht zwangsläufig in CPTs zu implementieren, sondern beispielsweise auf graphischer Basis in einer entsprechend gestalteten Anwendersoftware. So könnte ein Modell beispielsweise ähnlich zu der FN-FMEA im Stil von Fehlernetzen erstellt werden, während die Arithmetik der BN-Modelle hintergründig und rahmengebend die konsistente Grundlage zur Berechnung bildet. Damit erscheint es möglich, einen Ansatz, wie beispielsweise die probFMEA nach [Kaiser15] als Formalismus zur Modellierung zu verwenden. Dieser kann innerhalb eines entsprechend strukturhierarchischen und integralen Modellschemas, wie es in dieser Arbeit diskutiert wurde, als graphischer Formalismus zur Modellierung dienen. Mit diesem sind vorrangig nur ausdrücklich zu betrachtende Zusammenhänge explizit zu modellieren. Die Berechnung dieses Modells könnte nach dem integralen Modellschema mit dem Ansatz der BN erfolgen. Dabei ist die zuvor erläuterte Beschränkung auf die Modellierung ausschließlich alternativer Folgen zu beachten. Interessant wäre daher zudem eine Weiterentwicklung des Modellkonzepts beziehungsweise des Formalismus, durch die auch ein simultanes Auftreten mehrerer Folgesymptome intuitiv und konsistent darstellbar ist.

9 Zusammenfassung und Ausblick

In dieser Arbeit wurde das Schema probabilistischer Inferenznetzwerke zur Darstellung und Berechnung von Mehrzustands-Fehlermodellen in einem integralen und kohärenten Ansatz genutzt. Dazu wurde ein Rahmenkonzept für einen entsprechenden methodischen Ansatz zur Fehlermodellierung zusammengestellt. Anschließend erfolgte eine detaillierte Untersuchung der probabilistischen Arithmetik elementarer Netzwerkbeziehungen ausgehend von einer weiterentwickelten mengentheoretischen Anschauung des Schnitts mehrwertiger Zufallsgrößen. Damit erfolgten eine logische Interpretation der elementaren Einflussbeziehungen in Bayesschen Netzwerken (BN) sowie die Herleitung der dafür erforderlichen algebraischen Grundlagen. So konnte ein Ansatz verifiziert werden, mittels dessen komplexe System-Fehlermodelle als auf mehrwertigen Zufallsvariablen beruhende Netzwerke dargestellt werden können. Dieser diente darauffolgend zur Untersuchung der Verwendbarkeit von BN für strukturhierarchisch untergliederte integrale Modelle aus Fehlerursache- und Fehlerauswirkungsbeziehungen technischer Systeme. Dadurch wurde im Kontext des untersuchten Modellschemas gezeigt, wie hiermit komplexe und integrale System-Fehlermodelle auf Basis von BN implementiert und probabilistisch exakt ausgewertet werden können.

Im Zuge der Arbeit konnte gezeigt werden, wie integrale Mehrzustandsmodelle der Fehlerursache- und Auswirkungsbeziehungen für ein technisches System probabilistisch konsistent aufgebaut und ausgewertet werden können. Darüber hinaus wurde die in BN bestehende Möglichkeit zur Verwendung bedingter Folgewahrscheinlichkeiten in System-Fehlermodellen untersucht und verifiziert. Bei inhaltlicher Analogie zu FTA- und RBD-Modellen ermöglichen diese komplexeren Fehlermodelle jedoch eine präzisere, umfassendere und probabilistisch konsistente Abbildung des Systems. Im Vergleich zum bisherigen Stand der Wissenschaft und Technik stellt dieser Ansatz eine stärker differenzierbare und zugleich strukturell konsistente Grundlage für System-Fehlermodelle dar.

Die Auswertung der Fehlermodelle mittels der für BN verfügbaren exakten Lösungsalgorithmen konnte zudem validiert werden. Mit diesen ist die Auswertung entsprechender Fehlermodelle auch im Fall großer Modellumfänge und komplexer Abhängigkeitsbeziehungen mit akzeptablem Rechenaufwand möglich. Insgesamt bietet der Modellierungsansatz auf Basis von Netzwerken aus mehrwertigen Zufallsgrößen bislang nicht vorhandene Möglichkeiten zur gesamtheitlichen Fehleranalyse komplexer technischer Systeme. Dies wurde anhand einer Reihe vereinfachter Fallbeispiele verdeutlicht und diskutiert.

Die gebräuchliche Darstellung von BN ist für die Erstellung solcher Fehlermodelle jedoch nur in gewissen Grenzen bedingt durch Komplexität und Übersichtlichkeit geeignet. Dies erweist sich als maßgebliche Restriktion zur praktischen Anwendung des Modellierungsansatzes. Im Zuge der Arbeit wurden daher diverse Strategien zur optimierten Erfassung und Darstellung der im Modell verarbeiteten Informationen vorgeschlagen. Angesichts dieser ergonomischen Beschränkung wäre für die praktische Anwendung ein intuitiv erfassbares und aufwandsoptimiertes Bedien- und Darstellungskonzept wegweisend. Dies zielt vorrangig auf die Erleichterung der Bearbeitung der Fehlerbeziehungen gegenüber der gebräuchlichen Tabellenform sowie eine Aufwandsbeschränkung ab. Zudem wäre eine graphische Visualisierung der logischen Beziehungen zwischen einzelnen Fehlzuständen zur Verbesserung der Nachvollziehbarkeit günstig. Ferner könnten an mehreren Knoten einwirkende Größen, wie beispielsweise besondere Umgebungseinwirkungen oder Sicherheitsmechanismen in Anwenderprogrammen als spezifische Symbole an einzelnen Knoten lokal repräsentiert werden. Dies würde die Anzahl der vielfältigen und transversal zu den Strukturbeziehungen verlaufenden Netzverknüpfungen reduzieren, die andernfalls die Überschaubarkeit und Handhabbarkeit stark beeinträchtigen.

Ein Aspekt für Weiterentwicklungen von BN-Analysewerkzeugen wäre eine kontextspezifische Berechnungsumgebung, die die Ausfallwahrscheinlichkeiten zu einem gegebenen Zeitpunkt auf Basis von Berechnungsmodellen für die jeweiligen Komponenten auf der untersten Hierarchiestufe des Fehlermodells erlaubt. Darin wäre zudem eine Unterscheidung verschiedener Parametersätze für unterschiedliche Betriebsweisen und Umgebungsbedingungen umsetzbar. Eine wesentliche konzeptionelle Weiterentwicklung des Ansatzes dieser Arbeit wäre die Umsetzung integraler Fehlermodelle in zeitlich veränderlichen dynamischen BN. Dadurch könnten auch zeitliche Abhängigkeiten aufeinanderfolgender Fehlzustände probabilistisch verfeinert dargestellt werden. Ein weiterer Ansatz zur konzeptionellen Weiterentwicklung bestünde darin, auch simultane Fehlerfolgen probabilistisch geeignet abbilden zu können. Der grundlegende Ansatz in dieser Arbeit ist jedoch durch das Grundkonzept auf die Möglichkeit der Darstellung alternativer Fehlerfolgen, die sich gegenseitig ausschließen, beschränkt. Ein praktikabler Ansatz, der diese Restriktion überwindet, wäre zukunftsweisend für die praktische Anwendung.

Verzeichnisse

Literaturverzeichnis

[Almond92] Almond, R.G.: „An Extended Example for Testing GRAPHICAL-BELIEF." Statistic Science Research Report 6, Statistical Sciences Inc., Seattle, 1992.

[Arnauld72] Arnauld, A., Nicole, P.: „Die Logik oder die Kunst des Denkens". (Original: „La logique ou l'art de penser", Übers.: Axelos, C.), Ausgabe 2, Wissenschaftliche Buchgesellschaft, Darmstadt, 1972.

[Arroyo99] Arroyo-Figueroa, G., Sucar, L. E.: „A Temporal Bayesian Network for Diagnosis and Prediction". In: Proceedings of the 15th Conference on Uncertainty in Artificial Intelligence (UAI) pp. 13-19, Morgan Kaufmann Publishers Inc., 1999.

[Aven99] Aven, T., Jensen, U.: „Stochastic Models in Reliability". Springer, New York, 1999.

[Barlow65] Barlow, R. E., Proschan, F.: „Mathematical Theory of Reliability". Wiley, New York, 1965.

[Barlow78] R. E. Barlow, A. S. Wu: „Coherent systems with multistate components". Mathematics of Operations Research, Vol. 3(4), pp. 275-281, Institute for Operations Research and the Management Sciences (INFORMS), Linthicum, 1978:

[Barlow84] Barlow, R.E.: „Mathematical Theory of Reliability: A Historical Perspective". IEEE Transactions on Reliability, Vol. R-33(1), 1984.

[Barlow88] Barlow, R. E.: „Using influence diagrams". In: Clarotti, C. A., Lindley, D. V. (Hrsg.), Accelerated life testing and experts' opinions in reliability, Number 102, In: Enrico Fermi, International School of Physics, pp. 145–157. Elsevier Science Publishers B. V. (North-Holland), 1988.

[Barlow98] Barlow, R. E.: „Engineering Reliability". SIAM, Philadelphia, 1998.

[Bayes1763] Bayes, T., Price, R.: „An Essay towards solving a Problem in the Doctrine of Chances. By the late Rev. Mr. Bayes, communicated by Mr. Price, in a letter to John Canton, M. A. and F. R. S.". In: Philosophical Transactions of the Royal Society of London 53, pp., 370–418, 1763.

[Bazowsky61] Bazowsky, I.: „Reliability theory and practice". Prentice-Hall, Englewood Cliffs, 1961.

[Bertsche04] Bertsche, B., Lechner, G.: „Zuverlässigkeit im Fahrzeug und Maschinenbau". 3. Aufl., Springer, Berlin, 2004.

[Bertsche09] Bertsche, B., Göhner, P., Jensen, U., Schinköthe, W., Wunderlich, H.-J.: „Zuverlässigkeit mechatronischer Systeme: Grundlagen und Bewertung in frühen Entwicklungsphasen". Verband deutscher Ingenieure VDI (Hrsg.), Springer, Berlin, Heidelberg, 2009.

[BfS-Schr-37:05] BfS: „Methoden zur probabilistischen Sicherheitsanalyse für Kernkraftwerke“. Bundesamt für Strahlenschutz (BfS), Facharbeitskreis Probabilistische Sicherheitsanalyse für Kernkraftwerke, Wirtschaftsverlag NW / Verlag für neue Wissenschaft GmbH, Bremerhaven, 2005.

[Birolini14] Birolini, A.: „Reliability engineering: Theory and Practice“. Springer, Berlin, Heidelberg, 2014.

[Bobbio01] Bobbio, A., Portinale, L., Minichino, M., Ciancamerla, E.: „Improving the analysis of dependable systems by mapping fault trees into Bayesian networks“. In: Reliability Engineering and System Safety 71(3), pp. 249-260, Elsevier, 2001.

[Boissou03] Boissou, M., Pourret, O.: „A Bayesian Belief Network based Method for Performance evaluation and Troubleshooting of Multistate Systems”. In: International Journal of Reliability Quality and Safety Engineering, Vol. 10(4), pp. 407-416, 2003.

[Boole1847] Boole, G.: „The mathematical analysis of logic, being an essay towards a calculus of deductive reasoning“. Macmillan, Cambridge, 1847.

[Boudali04] Boudali, H., Dugan, J. B.: „A discrete-time Bayesian network reliability modeling and analysis framework“. In: Reliability Engineering and System Safety, Vol. 87 (2005), pp. 337-349, Elsevier, 2004.

[Boudali05] Boudali, H., Dugan, J. B.: „A New Bayesian Network Approach to Solve Dynamic Fault Trees". In: Annual Reliability and Maintainability Symposium (RAMS), pp. 451-456, IEEE, 2005.

[Boudali06] Boudali, H., Dugan, J. B.: „A Continuous-Time Bayesian Network Reliability Modeling, and Analysis Framework“. In: IEEE Transactions on Reliability, Vol. 55(1), IEEE, 2006.

[Bowles02] Bowles, J. B.: „Commentary - Caution: Constant Failure-Rate Models May Be Hazardous to Your Design“. IEEE Transactions on Reliability, Vol. 51(3), pp. 375-377, 2002.

[Bretthorst14] Bretthorst, L.: „Probability Theory As Extended Logic”. Washington University in St. Louis, 2014, URL: http://bayes.wustl.edu/, (Zugriff: 03.06.2016).

[Goble99] Goble, W. M., Brombacher, A. C.: „Using a failure modes, effects and diagnostic analysis (FMEDA) to measure diagnostic coverage in programmable electronic systems”. In: Reliability Engineering & System Safety, Vol. 66(2), pp. 145-148, 1999.

[Bromberg53] Bromberg, B. G.: „Reliability of Airborne Electronic Components”. In: Proceedings of the Institute of Radio Engineers, Vol. 41(4), pp. 513-516, IRE, 1953, (IEEE, 2007).

[Caldarola80] Caldarola, L.: "Coherent Systems with Multistate Components”. In: Nuclear Engineering and Design, Vol. 58(1), pp. 127-139, Elsevier North-Holland Publishing, 1980.

[Cantor1895] Cantor G.: „Beiträge zur Begründung der transfiniten Mengenlehre". In: Mathematische Annalen, Band 46(4), pp. 481–512, B. G. Teubner Verlag, Leipzig, 1895.

[Cao16] Cao, J., Yin, B., Lu, X.: „Probabilistic Risk Assessment of Multi-State Systems Based on Bayesian Networks". In: 18th International Conference on Advanced Communication Technology (ICACT), pp. 773 – 778, IEEE, 2016.

[Carhart53] Carhart, R. R.: „A Survey of the Current Status of the Electronic Reliability Problem". Research Memorandum 1131, RAND Corporation, Santa Monica, 1953.

[Carroll05] Carroll, J., Ruskey, F., Weston, M.: „Which n-Venn diagrams can be drawn with convex k-gons?". In: Proceedings of the Second International Workshop on Euler Diagrams (Euler 2005), Electronic Notes in Theoretical Computer Science, Elsevier, 2005.

[Castillo97] Castillo, E., Solares, C., Gómez, P.: „Tail uncertainty analysis in complex systems". In: Artificial Intelligence, Vol. 96 (2), pp. 395–419, Elsevier, 1997.

[Charniak91] Charniak, E.: „Bayesian Networks without Tears". In: AI Magazine, Vol. 12(4), AAAI, 1991.

[Chen10] Chen, G. B., Yang, Z.-C., Sun, Z.-H.: „Safety Analysis of Complex Systems based on Bayesian Networks". In: 2nd International Conference on Industrial Mechatronics and Automation (ICIMA), Vol. 1, pp.92-95, IEEE, 2010.

[Chorafas60] Chorafas, D.: „Statistical Processes and Reliability Engineering ". Van Nostrand Company Inc., Princeton, 1960.

[Chow97] Chow, C. S.: „Generating and Drawing Area-Proportional Euler and Venn Diagrams". Dissertation, Dept. of Computer Science, University of Victoria 1997.

[Couturat 1914] Couturat, L.: „The Algebra of Logic". Autorisierte Übersetzung aus dem Französischen, Open Court Publishing Company, Chicago, London, 1914.

[Darwiche02] Darwiche, A.: „A logical approach to factoring belief networks". In: Proceedings of Knowledge Representation (KR), pp. 409–420, Toulouse, 2002.

[Darwiche08] Darwiche, A.: „Handbook of Knowledge Representation, Chapter 11: Bayesian Networks". van Harmelen, F., Lifschitz, V. and Porter, B. (Hrsg.), Elsevier B. V., 2008.

[Dean89] Dean, T., Kanazawa, K.: „A Model for Reasoning about Persistence and Causation". In: Computational Intelligence, Vol. 5(2), pp. 142–150, Blackwell Publishers, Cambridge, 1989.

[DeLong70] DeLong, T. W.: „A Fault Tree Manual". Masterarbeit Texas A&M University, College Station, 1970.

[DGQ-Band17-10:02] DGQ: „DGQ Band 17-10: Zuverlässigkeitsmanagement – Einführung in das Management von Zuverlässigkeitsprogrammen". Deutsche Gesellschaft für Qualität e.V. DGQ, Beuth-Verlag, Berlin, 2002.

[DGQ-Band13-11:12] DGQ: „DGQ-Band13-11: FMEA - Fehlermöglichkeits- und Einflussanalyse". Deutsche Gesellschaft für Qualität e.V., Beuth-Verlag, Berlin, 2012.

[DIN-25419:85] DIN: „DIN 25419:1985: Ereignisablaufanalyse; Verfahren, graphische Symbole und Auswertung". Deutsches Institut für Normung DIN, Beuth Verlag, 1985.

[DIN-EN-60812:06] DIN (IEC): „DIN EN 60812:2006: Analysetechniken für die Funktionsfähigkeit von Systemen - Verfahren für die Fehlzustandsart- und -auswirkungsanalyse (FMEA)". Deutsches Institut für Normung DIN, Beuth Verlag, 2006.

[DIN-EN-61087:06] DIN (IEC): „DIN EN 61078:2006: Techniken für die Analyse der Zuverlässigkeit - Zuverlässigkeitsblockdiagramm und Boolesche Verfahren". Deutsches Institut für Normung DIN, Beuth Verlag, 2006.

[DIN-IEC-61025:07] DIN (IEC): „DIN-IEC-61025: Fehlzustandsbaumanalyse". Deutsches Institut für Normung DIN, Beuth Verlag, 2007.

[Dugan92] Dugan, J. B., Bavuso, S. J., Boyd, M. A.: „Dynamic Fault-Tree Models for Fault-Tolerant Computer Systems". In: IEEE Transactions on Reliability, Vol. 41(3), IEEE, 1992.

[Eckberg63] Eckberg, C.R., „WS-133B Fault Tree Analysis Program Plan". Boeing Company, Seattle, 1963.

[Ehrlenspiel 09] Ehrlenspiel, K.: „Integrierte Produktentwicklung". 4. Auflage, Hanser Verlag, 2009.

[El-Neweihi 78a] El-Neweihi, E., Proshan, F.: „Multistate Systems Reliability Models - A Survey". Technical Report, Department of Statistics, Kentucky University Lexington, 1978.

[Epstein05] Epstein, S., Rauzy, A.: „Can we trust PRA?". In: Reliability Engineering and System Safety, Vol. 88(3), pp. 195-205, Elsevier, 2005.

[Ericson99] Ericson, C. A. II: „Fault Tree Analysis – A History". In: Proceedings of the 17th International System Safety Conference, 1999.

[Euler1761] Euler, L.: „Lettres à une princesse d'allemagne. Sur divers sujets de physique et de philosophie". Vol. 2, Briefe Nr.102-108, Birkhauser, Basel, 1761.

[Feller50] Feller, W.: "An Introduction to Probability Theory and its Applications". Vol. 1, John Wiley, New York, 1950.

[Fitzpatrick75] Fitzpatrick, P. J.: „An Extension of Venn Diagrams". Notre Dame Journal of Formal Logic, Vol. XIV, Nr. 1, 1973.

[Frege1897] Frege, G.: „Begriffsschrift, eine der arithmetischen nachgebildete Formelsprache des reinen Denkens". Verlag Louis Nebert, Halle, 1879.

[Fry28] Fry, T. C.: „Probability and its engineering uses". D. Van Nostrand Company Inc., New York, 1928.

[García11] García, A., Gilabert, E.: „Mapping FMEA into Bayesian Networks". In: International Journal of Performability Engineering, Vol. 7(6), pp. 525-537, Totem Publisher Inc., 2011.

[Geiger88] Geiger, D., Pearl, J.: „On the Logic of Causal Models". In: Proceedings of the Fourth Annual Conference on Uncertainty in Artificial Intelligence (UAI '1988), pp. 3-14, Elsevier Science Publishers B.V. North Holland Publishing, 1990.

[GeNIe10] Decision Systems Laboratory, Softwareumgebung GeNIe 2.0 und SMILE, University of Pittsburgh, 2010, URL: https://dslpitt.org/genie, (Zugriff: 27.02.2015).

[Grunske07] Grunske, L., Colvin, R., Winter, K.: „Probabilistic Model-Checking Support for FMEA". In: Fourth International Conference on the Quantitative Evaluation of Systems, pp. 119-128, IEEE, 2007.

[Gurr98] Gurr, C., Lee, J., Stenning, K.: „Theories of Diagrammatic Reasoning: Distinguishing Component Problems". In: Minds and Machines, Vol. 8(4), pp. 533-557, Springer, 1998.

[Hamilton1863] Hamilton, W.: „Lectures on Logic, Lecture 14, Section II.- of the Products of Thought". In: Mansel, H. L.; Veitch, J. Lectures on Metaphysics and Logic, Gould and Lincoln, Boston, 1863.

[Hammer96] Hammer, E., Danner, N.: „Towards a Model Theory of Diagrams". In: Journal of Philosophical Logic, Vol. 25, pp. 463-482, Kluwer Academic Publishers, 1996.

[Hammer98] Hammer, E., Shin, S.-J.: „Euler's visual logic". In: History and Philosophy of Logic, Vol. 19(1), pp. 1-29, Taylor & Francis, 1998.

[Hitchkock10] Hitchcock, C.: „Probabilistic Causation". In: Stanford Encyclopedia of Philosophy, Center for the Study of Language and Information (CSLI), Stanford University, 2010, URL: https://plato.stanford.edu/entries/causation-probabilistic/#CauModeling, (Zugriff: 25.04.2017).

[IEC60050-192:15] IEC: „International Electrotechnical Vocabulary - Part 192: Dependability". International Electrotechnical Commission IEC, Genf, 2015.

[IEC61508:10] IEC: „Functional safety of electrical/electronic/programmable electronic safety-related systems". International Electrotechnical Commission (IEC), Genf, 2010.

[ISO26262:11] ISO: „Road vehicles - Functional safety". International Organization for Standardization (ISO), Genf, 2011.

[Jaynes03] Jaynes, E. T.: „Probability Theory: The Logic of Science". Cambridge University Press, 2003.

[Jensen94] Jensen, F. V., and Jensen, F.: „Optimal junction trees". In Proceedings of the lOth Conference on Uncertainty in Artificial Intelligence, pp. 360-366, Seattle, 1994.

[Jevons1888] Jevons, S.: „Elementary Lessons in Logic: Deductive and Inductive". Macmillan and Co., London, 1888.

[Kaiser03] Kaiser, B., Liggesmeyer, P., Mäckel, O.: „A New Component Concept for Fault Trees". In: P. A. Lindsay & A. Cant, (Hrsg.) SCS. CRPIT., pp. 37–46, Australian Computer Society, 2003.

[Kaiser06] Kaiser, B.: „Zustands-Ereignis-Fehlerbäume: Eine Sicherheits- und Zuverlässigkeitsanalysetechnik für softwaregesteuerte Systeme". Dissertation, Fachbereich Informatik, TU Kaiserslautern, 2006.

[Kaiser15] Kaiser, B., Rauschenbach, M.: „Probabilistic Extension of Failure Net Based FMEA". In: European Safety and Reliability Conference (ESREL 2015): Safety and Reliability of Complex Engineered Systems, pp. 1359-1366, CRC Press/Balkema, Taylor & Francis Group, 2015.

[Kempf01] Kempf, M.: „Failure Analysis with the Aid of Bayesian Networks". In: 6th annual International Conference on Industrial Engineering - Theory, Applications and Practice, International Journal of Industrial Engineering, San Francisco, 2001.

[Kempf08] Kempf, M.: „Ein Bayesscher Ansatz zur Bewertung technischer Risiken im Entwicklungsprozess". In: Informatik Forschung und Entwicklung 22, pp. 85-94, Springer, 2008.

[Khakzad11] Khakzad, N., Khan, F., Amyotte, P.: „Safety analysis in process facilities: Comparison of Fault tree and Bayesian network approaches". In: Reliability Engineering and System Safety, Vol. 96, pp. 925-932, Elsevier, 2011.

[Kim83] Kim, J. H., Pearl, J.: „A Computational Model for Causal and Diagnostic Reasoning in Inference Systems". In: Proceedings of the Eighth international joint conference on Artificial intelligence (IJCAI), Vol. 1, pp. 190-193, Morgan Kaufmann, 1983.

[Kim11] Kim, B., Vohnout, S., Mikkola, E., Li, M., Liu, J.: „Causal analysis for troubleshooting and decision support system". In: Conference on Prognostics and Health Management (PHM), pp. 1-7, IEEE, 2011.

[Kim14] Kim, B., Goodman, D., Li, M., Liu, J., Li, J.: „Improved Reliability-based Decision Support Methodology Applicable in System-level Failure Diagnosis and Prognosis". In: Transactions on Aerospace and Electronic Systems, Vol. 50(4), pp. 2630-2641, IEEE, 2014.

[Knight55] Knight, C. R., Jervis, E. R., Herd, G. R.: „The Definition of Terms of Interest in the Study of Reliability". Aeronautical Radio Inc., Washington, D. C., 1955.

[Kolmogorow 33] Kolmogorow, A. N.: „Grundbegriffe der Wahrscheinlichkeitstheorie". Springer, 1933.

[Kuznetsov94] Kuznetsov, N. Y.: „Fault Trees – Problems and the modern State of Investigations". In: Cybernetics and Systems Analysis 30(3), pp. 419-439, 1994, (veröffentlicht in: Kibernetika i Sistemnyi Analiz, No. 3, pp. 128-150, 1994).

[Lampis09] Lampis, M., Andrews, J. D.: „Bayesian Belief Networks for System Fault Diagnostics". Quality and Reliability Engineering International, Vol. 25, pp. 409-426, John Wiley & Sons, 2008.

[Lampis10] Lampis, M.: „Application of Bayesian Belief Networks to system fault diagnostics". Dissertation, Loughborogh University, 2010.

[Lange1712] Lange, J. C.: „Johannis Christiani Langii Nucleus logicae Weisianae". Johann Christian Lange (Hrsg.), Verlag H. Müller, 1712.

[Langseth07] Langseth, H., Portinale, L.: „Bayesian Networks in reliability". In: Reliability Engineering and System Safety, 92(1), pp. 92-108, Elsevier, 2007.

[Langseth08] Langseth, H.: „Bayesian Networks in Reliability: The Good, the Bad and the Ugly". Advances in Mathematical Modeling for Reliability, IOS Press, Amsterdam, 2008.

[Laplace1812] Marquis de Laplace, P. S.: „Théorie analytique des probabilités". Mme. Ve Courcier, Paris, 1812.

[Lauritzen88] Lauritzen, S. L., Spiegelhalter, D. J.: „Local Computation with Probabilities on Graphical Structures and Their Application to Expert Systems". In: Journal of the Royal Statistical Society Series B (Methodological), Vol. 50(2), pp. 157-224, Blackwell Publishing for the Royal Statistical Society, 1988.

[Lee01] Lee, B. H.: „Using Bayes Belief Networks in Industrial FMEA Modeling and Analysis". In: Proceedings of the annual Reliability and Maintainability Symposium (RAMS), 2001.

[Lee02] Lee, B. H.: „Failure modes and effects analysis with Bayesian belief networks: bridging the design-diagnosis modeling gap". Dissertation Stanford University, Palo Alto, 2002.

[Lee85] Lee, W. S., Grosh, D. L., Tillman, F. A., Lie, C. H.: „Fault Tree Analysis, Methods, and Applications - A Review". In: Transactions on Reliability, Vol. R-34(3), pp. 194-203, IEEE, 1985.

[Lee99a] Lee, B. H.: „Encoding Design FMEA Causal Models As Bayesian Network Structures". In: Proceedings of the International Conference on Engineering Design (IECD 99), München, 1999.

[Lee99b] Lee, B. H.: „Design FMEA for Mechatronic Systems using Bayesian Network Causal Models". In: Proceedings of the 1999 ASME Design Engineering Technical Conferences, Las Vegas, 1999.

[Leyendecker 08] Leyendecker, H.-W.: "VDMA Kennzahlen Entwicklung und Konstruktion". Verein Deutscher Maschinen und Anlagenbau e. V. (VDMA), VDMA-Verlag, Frankfurt Main, 2008.

[Lisnianski10] Lisnianski, A., Frenkel, I., Ding, Y.: „Multi-state System Reliability Analysis and Optimization for Engineers and Industrial Managers". Springer, London, 2010.

[Mahadevan 01] Mahadevan, S., Zhang, R., Smith, N.: „Bayesian Networks for System Reliability Reassessment". In: Structural Safety, Vol. 23, pp. 231-251, Elsevier, 2001.

[Marca88] Marca, D. A., McGowan, L.: „SADT – Structured Analysis and Design Technique". McGraw Hill, New York, 1988.

[Marquez10] Marquez, D., Neil, M., Fenton, N.: „Improved reliability modeling using Bayesian networks and dynamic discretization". In: Reliability Engineering & System Safety, Volume 95(4), pp. 412-425, Elsevier, 2010.

[Mateescu10] Mateescu, R., Kask, K., Gogate, V., Dechter, R.: „Join-Graph Propagation Algorithms". In: Journal of Artificial Intelligence Research, Vol. 37, pp. 279-328, 2010.

[Mi12] Mi, J., Li, Y., Huang, H.-Z., Liu, Y., Zhang, X.: „Reliability Analysis of Multi-State Systems With Common Cause Failure Based on Bayesian Networks". In: International Conference on Quality, Reliability, Risk, Maintenance and Safety Engineering (ICQR2MSE), 2012.

[MIL-HDBK 338B:98] U. S. Department of Defence: „Military Handbook 338 B: Electronic Reliability Design Handbook". U. S. Department of Defence, Washington, 1998.

[MIL-STD-1629A:80] U. S. Department of Defence: „MIL-STD 1629A - Military Standard Procedures for Performing a Failure Mode, Effects and Criticality Analysis (AMSC N3074)". U. S. Department of Defence, Washington, 1980.

[Misra08] Misra, K. B.: „The Handbook of Performability Engineering". Springer, London, 2008.

[Montani05] Montani, S., Portinale, L., Bobbio, A.: „Dynamic Bayesian Networks for modeling advanced Fault Tree features in Dependability Analysis". In: Proceedings of the sixteenth European Conference on Safety and Reliability, 2005.

[Moore56] Moore, E. F., Shannon, C.E.: „Reliable circuits using less reliable relay". In: Journal of the Franklin Institute, Vol. 262(3), pp. 191-208 und Vol. 262(4), pp. 281-297, 1956.

[Murphy02] Murphy, K.: „Dynamic Bayesian Networks: Representation, Inference and Learning". Dissertation, UC Berkeley, Computer Science Division, 2002.

[Murphy98] Murphy, K.: „A Brief Introduction to Graphical Models and Bayesian Networks". University of British Columbia, 1998, URL: www.cs.ubc.ca/~murphyk/Bayes /bnintro.html, (Zugriff: 31.05.2016).

[NASA-STD-8729.1:98] National Aeronautics and Space Administration, NASA: „Planning, Developing and Managing an effective Reliability and Maintainability (R&M) Program". NASA Technical Standard NASA-STD-8729.1, Washington, 1998.

[Natvig11] Natvig, B.: „Multistate Systems Reliability Theory with Applications". John Wiley and Sons ltd, 2011.

[El-Neweihi78b] El-Neweihi, E., Proschan, F., Sethuraman, J.: „Multistate coherent systems". In: Journal of Applied Probability, Vol. 15(4), pp. 675-688, Applied Probability Trust, 1978.

[Peano1888] Peano, G.: „Calculo Geometrico secondo l'Ausdehnungslehre di H. Grassmann preceduto dalle operazioni della logica deduttiva". Fratelli Bocca Editori, Turin, 1888.

[Pearl00] Pearl, J.: „Causality: models, reasoning, and inference". Cambridge Univ. Press, Cambridge, 2000.

[Pearl82] Pearl, J.: „Reverend Bayes on Inference Engines: A Distributed Hierarchical Approach". In: Proceedings of the American Association of Artificial Intelligence National Conference on Artificial Intelligence, pp. 133-136, Pittsburgh, 1982.

[Pearl85] Pearl, J.: „Bayesian Networks: A Model of Self-Activated Memory for Evidential Reasoning". Seventh Annual Conference of the Cognitive Science Society, 1985.

[Pearl88] Pearl, J.: „Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference". Series in Representation and Reasoning, Morgan Kaufmann, 1988.

[Pfeiffer65] Pfeiffer, P. E.: „Concepts of Probability Theory". McGraw-Hill, New York, 1965.

[Pickard05] Pickard, K., Müller, P. & Bertsche, B.: „Multiple failure mode and effects analysis – an approach to risk assessment of multiple failures with FMEA". In: Proceedings of the Annual Reliability and Maintainability Symposium RAMS, pp. 457–462., IEEE, 2005.

[Poon11] Poon, H., Domingos, P.: „Sum-Product Networks: A New Deep Architecture". In: International Conference on Computer Vision Workshops (ICCV) pp. 689-690, IEEE, 2011.

[Portinale99] Portinale, L., Bobbio, A.: „Bayesian Networks for Dependability Analysis: An Application to Digital Control Reliability". In: Proceedings of the 15th Conference on Uncertainty in Artificial Intelligence (UAI), pp. 551-558, Morgan Kaufman, 1999.

[Portinale05] Portinale L, Bobbio A, Montani S.: „From AI to Dependability: using Bayesian Networks for Reliability Modeling and Analysis". In: Wilson, A. G., Limnios, N., Keller-McNulty, S. A., Armijo Y. M., (Hrsg.), Modern Statistical and Mathematical Methods in Reliability, pp. 365–381, World Scientific, 2005.

[Portinale10] Portinale, L., Raiteri, C. D., Montani, S.: „Supporting reliability engineers in exploiting the power of Dynamic Bayesian Networks". In: International Journal of Approximate Reasoning, Vol. 51'(2), pp. 179-195, Elsevier, 2010.

[Portinale15] Portinale, L., Codetta Raiteri, D.: „Modeling and Analysis of Dependable Systems: A Probabilistic Graphical Model Perspective". World Scientific, 2015.

[Price98] Price, C., Taylor, N.: „FMEA for Multiple Failures". In: Proceedings of the Annual Reliability and Maintainability Symposium, pp. 43-47, International Symposium on Product Quality and Integrity, Anaheim, 1998.

[Rakowsky01] Rakowsky, U. K.: „System-Zuverlässigkeit: Terminologie, Methoden, Konzepte". LiLoLe, Hagen, 2001.

[Rausand04] Rausand, M., Høyland, A.: „System Reliability Theory: Models, Statistical Methods and Applications". John Wiley, 2004.

[Rauschenbach15] Rauschenbach, M., Nuffer, J., Mayer, D.: „Probabilistische Systemfehler- und Zuverlässigkeitsanalyse auf Basis von FMEA und hierarchischen Bayes-Netzwerken". In: 27. Fachtagung Technische Zuverlässigkeit (TTZ), Verein Deutscher Ingenieure (VDI), Leonberg, 2015.

[Ruijters15] Ruijters, E., Stoelinga, M.: „Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools". In: Journal of Computer Science Review archive, Vol. 15(C), pp. 29-62, Elsevier Science Publishers B. V. Amsterdam, 2015.

[Russell95] Russell, S., Norvig, P.: „Artificial Intelligence: A Modern Approach". Prentice Hall, Englewood, 1995.

[Shin91] Shin, S.-J.: „A Situation-Theoretic Account of Valid Reasoning with Venn Diagrams". In: J. Barwise et al. (Hrsg.): Situation Theory and Its Applications, Vol. 2., Stanford: CSLI, 1991.

[Shin94] Shin, S.-J.: „The Logical Status of Diagrams". Cambridge University Press, 1994.

[Simon07] Simon, C., Weber, P., Levrat, E.: „Bayesian Networks and Evidence Theory to Model Complex Systems Reliability". In: Journal of Computers, Vol. 2 (1), pp. 33-43, 2007.

[Smith11] Smith, D.: „Reliability, Maintainability and Risk: Practical Methods for Engineers". Butterworth-Heinemann, 8. Aufl., 2011.

[Stapelberg 09] Stapelberg, R. F.: „Handbook of reliability, availability, maintainability and safety in engineering design". Springer, London, 2009.

[Stapleton05] Stapleton, G.: „A Survey of Reasoning Systems Based on Euler Diagrams". In: Electronic Notes in Theoretical Computer Science, Vol. 134, pp. 127–151, Elsevier, 2005.

[Swoboda97] Swoboda, N. G.: „Implementing Euler/Venn Reasoning Systems". AAAI Technical Report FS-97-03. In: Reasoning with Diagrammatic Representations II Symposium, AAAI Press, Menlo Park, 1997.

[Swoboda02] Swoboda, N., Allwein, G.: „Using DAG Transformations to verify Euler/Venn homogeneous and Euler/Venn FOL heterogeneous Rules of Inference". In: First International Conference on Graph Transformation and Visual Modeling Techniques 2002, Electronic Notes in Theoretical Computer Science, Vol. 72(3), pp. 78-92, Elsevier, 2003.

[Swoboda05] Swoboda, N., Allwein, G.: „Heterogeneous Reasoning with Euler/Venn Diagrams Containing Named Constants and FOL". In: Electronic Notes in Theoretical Computer Science, Vol. 134, pp. 153–187, 2005.

[Torres98] Torres Toledano, J. G., Sucar, L. E.: „Bayesian Networks for Reliability Analysis of Complex Systems". Kapitel in: Lecture Notes in Computer Science, Vol. 1484. In: Proceedings of the 6th Ibero-American conference on AI: Progress in Artificial Intelligence, pp. 195-206, Lissabon, 1998.

[VDA-Band3:04] VDA: „VDA Band 3 Teil 02: Zuverlässigkeitssicherung bei Automobilherstellern und Lieferanten: Zuverlässigkeits- Methoden und –Hilfsmittel". Verband der Automobilindustrie e.V., 3. Aufl., VDA, Frankfurt am Main, 2000, aktualisiert 2004.

[VDA-Band4-FMEA:06] VDA: „Band 4, Kapitel: Produkt- und Prozess FMEA". Verband der Automobilindustrie VDA, Frankfurt Main, (2.Aufl., akt. 2012) 2006.

[VDA-Band4:03] VDA: „Band 4, Qualitätsmanagement in der Automobilindustrie - Sicherung der Qualität vor Serieneinsatz". Verband der Automobilindustrie VDA (4. Aufl.), Frankfurt Main, 2003.

[VDI-2206:04] VDI: „VDI-Richtlinie 2206: Entwicklungsmethodik für mechatronische Systeme". Verein Deutscher Ingenieure e.V., Düsseldorf, 2004.

[VDI4003:07] VDI: „Zuverlässigkeitsmanagement". Verein Deutscher Ingenieure VDI e. V., Beuth Verlag, 2007.

[Venn1880] Venn, J.: „On the Diagrammatic and Mechanical Representation of Propositions and Reasonings.". London, Edinburgh and Dublin Philosophical Magazine and Journal of Science, Vol. X. Fifth Series, pp. 1-18, Taylor and Francis, London, 1880.

[Vesely02] Vesely, W., Stamatelatos, M., Dugan, J., Fragola, J., Minarick, J., Railsback, J.: „Fault Tree Handbook with Aerospace Applications". NASA Office of Safety and Mission Assurance NASA Headquarters, Washington, 2002.

[Vesely81] Vesely, W. E., Goldberg, F. F., Roberts, N. H., Haasl, D. F.: „Fault Tree Handbook". U.S. Nuclear Regulatory Commission, Washington DC, 1981.

[Watson62] Watson, H. A.: „Launch Control Safety Study Vol. I and II". Bell Telephone Laboratories, Murray Hill, 1962.

[Weber03] Weber, P., Jouffe, L.: „Reliability modelling with dynamic Bayesian networks". In: 5th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes (SAFEPROCESS), Washington DC, 2003.

[Weber06] Weber, P., Jouffe, L.: „Complex system reliability modelling with Dynamic Object Oriented Bayesian Networks (DOOBN)". In: Reliability Engineering and System Safety, 91(2), pp. 149-162, Elsevier, 2006 .

[Weber12] Weber, P., Medina-Oliva, G., Simon, C., Iung, B.: „Overview on Bayesian networks Applications for Dependability, Risk Analysis and Maintenance areas". In: Engineering Applications of Artificial Intelligence, Vol. 25(4), pp. 671-682, Elsevier, 2012.

[Werdich12] Werdich, M.: „FMEA - Einführung und Moderation". Werdich, M. (Hrsg.), Springer Vieweg, 2012.

[Whittaker90] Whittaker, J.: „Graphical Models in Applied Multivariate Statistics". Wiley Publishing, New York, 2009.

[Wood83] Wood, A. P.: „Multistate Reliability". Department of Operations Research and Department of Statistics, Stanford University, 1983.

[Wood85] Wood, A. P.: „Multistate Block Diagrams and Fault Trees". In: IEEE Transactions on Reliability, Vol. R-34(3), pp. 236-240, IEEE.

[Xiao11] Xiao, N. et al.: „Multiple failure modes analysis and weighted risk priority number evaluation in FMEA". In: Engineering Failure Analysis, Vol. 18(4), pp. 1162–1170, Elsevier, 2011.

[Xizhi84] Xizhi, H.: „The generic method of the multistate fault tree analysis". In: Microelectronics Reliability, Vol. 24(4), pp. 617-622, Elsevier, 1984.

[Yingkui12] Yingkui, G., Jing, L.: „Multi-State System Reliability: A New and Systematic Review". In: International Workshop on Information and Electronics Engineering, Procedia Engineering, Vol. 29, pp. 531-536, Elsevier, 2012.

[Zhai13] Zhai, S., Lin, S.: „Bayesian Networks Application in Multi-State System Reliability Analysis". In: Proceedings of the 2nd International Symposium on Computer, Communication and Automation (ISCCCA) Vols. 347-350, pp. 2590-2595, Atlantis Press, Paris, 2013.

[Zhou06] Zhou, Z., Jin, G., Dong, D., Zhou, J.: „Reliability Analysis of Multistate Systems Based on Bayesian Networks". In: 13th Annual IEEE International Symposium and Workshop on Engineering of Computer-Based Systems (ECBS'06), IEEE, 2006.

[Zocher05] Zocher, A.: „Quantitative Auswertung von Multizustand-Komponentenfehlerbäumen durch mehrwertige Entscheidungsdiagramme“. Masterarbeit, Hasso-Plattner-Institut für Softwaresystemtechnik an der Universität Potsdam, 2005.

Abbildungsverzeichnis

Tabellenverzeichnis